

# PATENT COOPERATION TREATY

PCT

## NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

From the INTERNATIONAL BUREAU

To:  
MITSUBISHI MATERIALS CORPORATION  
Intellectual Property Dept.  
6-1, Ohtemachi 1-chome  
Chiyoda-ku  
Tokyo 100-0004  
JAPON

|   |  |  |  |
|---|--|--|--|
| Date of mailing (day/month/year)<br>25 November 1999 (25.11.99) |  | IMPORTANT NOTICE   |  |
| Applicant's or agent's file reference<br>98P30155               |  |  |  |
| International application No.<br>PCT/JP99/02510                 | International filing date (day/month/year)<br>14 May 1999 (14.05.99) | Priority date (day/month/year)<br>18 May 1998 (18.05.98) |  |
| Applicant<br>MITSUBISHI MATERIALS CORPORATION et al             |  |  |  |

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:  
EP,US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:  
None

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on 25 November 1999 (25.11.99) under No. WO 99/60749

### REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a demand for international preliminary examination must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

### REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the national phase, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

|   |                                 |
|---|---------------------------------|
| The International Bureau of WIPO<br>34, chemin des Colombettes<br>1211 Geneva 20, Switzerland | Authorized officer<br>J. Zahra  |
| Facsimile No. (41-22) 740.14.35   | Telephone No. (41-22) 338.83.38 |

2960622

This Page Blank (uspto)

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/02510

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>6</sup> H04L9/08, H04L9/32, G09C1/00, G06F15/40

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>6</sup> H04L9/08, H04L9/32, G09C1/00, G06F15/40

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1999

Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
|-----------|--|-----------------------|
| Y         | Masahiro Mitsuyasu, Eiji Okamoto, "Kagi haisou, kagi kanri to ninshou" bit, Vol. 28, No. 8 (8. 1996) Pages 87 to 95                                    | 1-17, 51-60           |
| Y         | APPLIED CRYPTOGRAPHY SECOND EDITION, ✓<br>"3.1 Key Exchange" (U.S.)<br>John Wiley & Sons, Inc., (1996) Pages 47 to 52                                  | 1-17, 51-60           |
| Y         | JP, 10-13403, A (NEC Corp.), ✓<br>16 January, 1998 (16. 01. 98),<br>Full text ; Figs. 1 to 7 (Family: none)  | 18-106                |
| Y         | JP, 7-200617, A (Nippon Telegraph & Telephone Corp.),<br>4 August, 1995 (04. 08. 95),<br>Full text ; Figs. 1 to 9 (Family: none)                       | 18-27, 61-68          |
| Y         | JP, 10-40155, A (Fujitsu Ltd.), ✓<br>13 February, 1998 (13. 02. 98),<br>Par. Nos. [0022] to [0024], [0027] to [0030] ;<br>Figs. 1 to 15 (Family: none) | 18-60, 96-106         |

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

|   |  |
|---|--|
| * Special categories of cited documents:  | "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  |
| "A" document defining the general state of the art which is not considered to be of particular relevance  | "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone   |
| "E" earlier document but published on or after the international filing date  | "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" document member of the same patent family  |
| "O" document referring to an oral disclosure, use, exhibition or other means  |  |
| "P" document published prior to the international filing date but later than the priority date claimed  |  |

Date of the actual completion of the international search  
18 August, 1999 (18. 08. 99)Date of mailing of the international search report  
31 August, 1999 (31. 08. 99)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

**This Page Blank (uspto)**



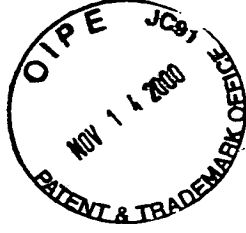
## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/02510

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
|-----------|--|-----------------------|
| Y         | JP, 7-245605, A (Fujitsu Ltd.),<br>19 September, 1995 (19. 09. 95),<br>Full text ; Figs. 1 to 10<br>& GB, 2287160, A & US, 5642420, A                  | 73-91                 |
| Y         | JP, 9-252323, A (Sony Corp.), /<br>22 September, 1997 (22. 09. 97),<br>Par. Nos. [0028] to [0033] ; [0040] to [0052] ;<br>Figs. 1 to 10 (Family: none) | 28-50, 78-91          |



This Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/02510

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>6</sup> H04L9/08, H04L9/32, G09C1/00, G06F17/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>6</sup> H04L9/08, H04L9/32, G09C1/00, G06F17/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1999

Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages  | Relevant to claim No. |
|-----------|---|-----------------------|
| Y         | Masahiro Mitsuyasu, Eiji Okamoto, "Kagi haisou, kagi kanri to ninshou" bit, Vol. 28, No. 8 (8. 1996) Pages 87 to 95                         | 1-17, 51-60           |
| Y         | APPLIED CRYPTOGRAPHY SECOND EDITION, "3.1 Key Exchange" (U.S.) John Wiley & Sons, Inc., (1996) Pages 47 to 52                               | 1-17, 51-60           |
| Y         | JP, 10-13403, A (NEC Corp.), 16 January, 1998 (16. 01. 98), Full text ; Figs. 1 to 7 (Family: none)   | 18-106                |
| Y         | JP, 7-200617, A (Nippon Telegraph & Telephone Corp.), 4 August, 1995 (04. 08. 95), Full text ; Figs. 1 to 9 (Family: none)                  | 18-27, 61-68          |
| Y         | JP, 10-40155, A (Fujitsu Ltd.), 13 February, 1998 (13. 02. 98), Par. Nos. [0022] to [0024], [0027] to [0030] ; Figs. 1 to 15 (Family: none) | 18-60, 96-106         |

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

|   |  |
|---|--|
| * Special categories of cited documents:  | "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  |
| "A" document defining the general state of the art which is not considered to be of particular relevance  | "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone   |
| "E" earlier document but published on or after the international filing date  | "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" document member of the same patent family  |
| "O" document referring to an oral disclosure, use, exhibition or other means  |  |
| "P" document published prior to the international filing date but later than the priority date claimed  |  |

Date of the actual completion of the international search  
18 August, 1999 (18. 08. 99)

Date of mailing of the international search report  
31 August, 1999 (31. 08. 99)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/JP99/02510

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
|-----------|--|-----------------------|
| Y         | JP, 7-245605, A (Fujitsu Ltd.),<br>19 September, 1995 (19. 09. 95),<br>Full text ; Figs. 1 to 10<br>& GB, 2287160, A & US, 5642420, A                | 73-91                 |
| Y         | JP, 9-252323, A (Sony Corp.),<br>22 September, 1997 (22. 09. 97),<br>Par. Nos. [0028] to [0033] ; [0040] to [0052] ;<br>Figs. 1 to 10 (Family: none) | 28-50, 78-91          |

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>6</sup> H04L9/08, H04L9/32, G09C1/00, G06F17/30

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>6</sup> H04L9/08, H04L9/32, G09C1/00, G06F17/30

最小限資料以外の資料で調査を行った分野に含まれるもの

|             |            |
|-------------|------------|
| 日本国実用新案公報   | 1922-1996年 |
| 日本国公開実用新案公報 | 1971-1999年 |
| 日本国登録実用新案公報 | 1994-1999年 |
| 日本国実用新案登録公報 | 1996-1999年 |

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

| 引用文献の<br>カテゴリー* | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示   | 関連する<br>請求の範囲の番号 |
|-----------------|---|------------------|
| Y               | 満保 雅浩, 岡本 栄司, "鍵配送、鍵管理と認証"<br>bit, Vol. 28, No. 8 (8. 1996) 第87-95頁                                       | 1-17, 51-60      |
| Y               | APPLIED CRYPTOGRAPHY SECOND EDITION,<br>"3.1 Key Exchange" (米)<br>John Wiley & Sons, Inc., (1996) 第47-52頁 | 1-17, 51-60      |
| Y               | JP, 10-13403, A (日本電気株式会社)<br>16. 1月. 1998 (16. 01. 98)<br>全文, 第1-7図 (ファミリーなし)                            | 18-106           |

☒ C欄の続きにも文献が列举されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献  
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

18. 08. 99

国際調査報告の発送日

31.08.99

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)  
郵便番号100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5W

4229

電話番号 03-3581-1101 内線 3576

| C (続き) . 関連すると認められる文献 |   |                  |
|-----------------------|---|------------------|
| 引用文献の<br>カテゴリー*       | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示   | 関連する<br>請求の範囲の番号 |
| Y                     | JP, 7-200617, A (日本電信電話株式会社)<br>4. 8月. 1995 (04. 08. 95)<br>全文, 第1-9図 (ファミリーなし)   | 18-27, 61-68     |
| Y                     | JP, 10-40155, A (富士通株式会社)<br>13. 2月. 1998 (13. 02. 98)<br>第 [0022] - [0024] 段落, 第 [0027] - [0030] 段落,<br>第1-15図 (ファミリーなし) | 18-60, 96-106    |
| Y                     | JP, 7-245605, A (富士通株式会社)<br>19. 9月. 1995 (19. 09. 95)<br>全文, 第1-10図<br>& GB, 2287160, A & US, 5642420, A                 | 73-91            |
| Y                     | JP, 9-252323, A (ソニー株式会社)<br>22. 9月. 1997 (22. 09. 97)<br>第 [0028] - [0033] 段落, 第 [0040] - [0052] 段落,<br>第1-10図 (ファミリーなし) | 28-50, 78-91     |

3T

## 特 許 協 力 条 約

PCT

REC'D 12 SEP 2000

WIPO

PCT

## 国際予備審査報告

(法第12条、法施行規則第56条)  
〔PCT36条及びPCT規則70〕

|  |   |                         |
|--|---|-------------------------|
| 出願人又は代理人<br>の書類記号 98P30155   | 今後の手続きについては、国際予備審査報告の送付通知（様式PCT/<br>IPEA/416）を参照すること。 |                         |
| 国際出願番号<br>PCT/JP99/02510   | 国際出願日<br>(日.月.年) 14.05.99                             | 優先日<br>(日.月.年) 18.05.98 |
| 国際特許分類 (IPC)<br>Int. Cl <sup>7</sup> H04L9/08, H04L9/32, G09C1/00, G06F17/30 |   |                         |
| 出願人 (氏名又は名称)<br>三菱マテリアル株式会社  |   |                         |

1. 国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条 (PCT36条) の規定に従い送付する。
2. この国際予備審査報告は、この表紙を含めて全部で 6 ページからなる。
- ☐ この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び/又はこの国際予備審査機関に対してした訂正を含む明細書、請求の範囲及び/又は図面も添付されている。  
(PCT規則70.16及びPCT実施細則第607号参照)  
この附属書類は、全部で ページである。
3. この国際予備審査報告は、次の内容を含む。
- I ☒ 国際予備審査報告の基礎
  - II ☐ 優先権
  - III ☐ 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
  - IV ☐ 発明の単一性の欠如
  - V ☒ PCT35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
  - VI ☐ ある種の引用文献
  - VII ☐ 国際出願の不備
  - VIII ☐ 国際出願に対する意見

|  |  |         |
|--|--|---------|
| 国際予備審査の請求書を受理した日<br>16.12.99                                     | 国際予備審査報告を作成した日<br>18.08.00                             |         |
| 名称及びあて先<br>日本国特許庁 (IPEA/JP)<br>郵便番号100-8915<br>東京都千代田区霞が関三丁目4番3号 | 特許庁審査官 (権限のある職員)<br>青木 重徳<br>電話番号 03-3581-1101 内線 3574 | 5W 4229 |

様式PCT/IPEA/409 (表紙) (1998年7月)

This Page Blank (uspto)



## I. 国際予備審査報告の基礎

1. この国際予備審査報告は下記の出願書類に基づいて作成された。(法第6条(PCT 14条)の規定に基づく命令に応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。  
PCT規則70.16, 70.17)

☒ 出願時の国際出願書類

- |                                     |         |        |                       |
|-------------------------------------|---------|--------|-----------------------|
| <input type="checkbox"/> 明細書        | 第 _____ | ページ、   | 出願時に提出されたもの           |
| <input type="checkbox"/> 明細書        | 第 _____ | ページ、   | 国際予備審査の請求書と共に提出されたもの  |
| <input type="checkbox"/> 明細書        | 第 _____ | ページ、   | _____ 付の書簡と共に提出されたもの  |
| <input type="checkbox"/> 請求の範囲      | 第 _____ | 項、     | 出願時に提出されたもの           |
| <input type="checkbox"/> 請求の範囲      | 第 _____ | 項、     | PCT 19条の規定に基づき補正されたもの |
| <input type="checkbox"/> 請求の範囲      | 第 _____ | 項、     | 国際予備審査の請求書と共に提出されたもの  |
| <input type="checkbox"/> 請求の範囲      | 第 _____ | 項、     | _____ 付の書簡と共に提出されたもの  |
| <input type="checkbox"/> 図面         | 第 _____ | ページ/図、 | 出願時に提出されたもの           |
| <input type="checkbox"/> 図面         | 第 _____ | ページ/図、 | 国際予備審査の請求書と共に提出されたもの  |
| <input type="checkbox"/> 図面         | 第 _____ | ページ/図、 | _____ 付の書簡と共に提出されたもの  |
| <input type="checkbox"/> 明細書の配列表の部分 | 第 _____ | ページ、   | 出願時に提出されたもの           |
| <input type="checkbox"/> 明細書の配列表の部分 | 第 _____ | ページ、   | 国際予備審査の請求書と共に提出されたもの  |
| <input type="checkbox"/> 明細書の配列表の部分 | 第 _____ | ページ、   | _____ 付の書簡と共に提出されたもの  |

2. 上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である \_\_\_\_\_ 語である。

- ☐ 国際調査のために提出されたPCT規則23.1(b)にいう翻訳文の言語  
☐ PCT規則48.3(b)にいう国際公開の言語  
☐ 国際予備審査のために提出されたPCT規則55.2または55.3にいう翻訳文の言語

3. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

- ☐ この国際出願に含まれる書面による配列表  
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表  
☐ 出願後に、この国際予備審査(または調査)機関に提出された書面による配列表  
☐ 出願後に、この国際予備審査(または調査)機関に提出されたフレキシブルディスクによる配列表  
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった  
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

4. 補正により、下記の書類が削除された。

- ☐ 明細書 第 \_\_\_\_\_ ページ  
☐ 請求の範囲 第 \_\_\_\_\_ 項  
☐ 図面 図面の第 \_\_\_\_\_ ページ/図

5. ☐ この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。(PCT規則70.2(c) この補正を含む差し替え用紙は上記1.における判断の際に考慮しなければならない、本報告に添付する。)

*This Page Blank (uspto)*

V. 新規性、進歩性又は産業上の利用可能性についての法第12条(PCT35条(2))に定める見解、それを裏付ける文献及び説明

1. 見解

|               |       |       |   |
|---------------|-------|-------|---|
| 新規性(N)        | 請求の範囲 | 1-106 | 有 |
|               | 請求の範囲 |       | 無 |
| 進歩性(IS)       | 請求の範囲 |       | 有 |
|               | 請求の範囲 | 1-106 | 無 |
| 産業上の利用可能性(IA) | 請求の範囲 | 1-106 | 有 |
|               | 請求の範囲 |       | 無 |

2. 文献及び説明(PCT規則70.7)

請求の範囲: 1-17

文献1: 満保 雅浩, 岡本 栄司; “鍵配送、鍵管理と認証”

bit, Vol. 28, No. 8 (8月, 1996) 第87-95頁  
には、メッセージ毎にランダムに発生する鍵を公開鍵暗号により暗号化すると共に、公開鍵証明書や電子署名を付加してデータや送信者の正当性を補償しつつ配送することで、通信当事者間で前記メッセージ毎にランダムに発生する鍵を安全に共有できるプロトコルが記載されている。

文献2: APPLIED CRYPTOGRAPHY  
(SECOND EDITION)

John Wiley & Sons, Inc. 発行, (1996)

“3.1 Key Exchange” 第47-52頁

には、公開鍵を登録してあるセンタによるセッション鍵の鍵共有プロトコルと、該プロトコルに対する複数の攻撃方法が記載されている。

文献3: JP, 9-212089, A (松下電器産業株式会社)

15. 8月, 1997 (15. 08. 97) 全文, 図1-12

には、特定グループ内でのメンバー変更に応じてグループ公開鍵を更新し、このグループ公開鍵を用いてグループの各メンバー端末に対して新たな鍵を同報配布する技術が記載されている。

各種攻撃に対する鍵の安全な配送、共有を実現するために、文献1に記載されている公開鍵証明書や電子署名を付加してデータや送信者の正当性を補償しつつ文献2, 3に記載されている鍵の配送、共有を行うことは、当該技術分野の専門家にとっては自明のものである。

請求の範囲: 18-27

文献4: JP, 10-13403, A (日本電気株式会社)

16. 1月, 1998 (16. 01. 98) 全文, 第1-7図

には、情報データと、該情報データを暗号化した署名データと、該署名データの作成に用いた暗号キーの検証データとをデータベースにて保管し、利用者は前記情報データを前記検証データで暗号化した結果を前記署名データと比較することで検証が可能とする技術が記載されている。

文献5: JP, 7-200617, A (日本電信電話株式会社)

4. 8月, 1995 (04. 08. 95) 全文, 第1-9図

には、データベース上の保存情報を参照権限のある複数ユーザで共有する技術が記載されている。

文献6: JP, 10-40155, A (富士通株式会社)

**This Page Blank (uspto)**

補充欄 (いずれかの欄の大きさが足りない場合に使用すること)

## 第 V. 2 欄の続き

22. 2月. 1998 (13. 02. 98)

第【0022】-【0024】段落,

第【0027】-【0030】段落, 第1-15図

には、データベースにアクセス権限管理ユニットを設け、グループ定義体に基づく利用者帰属情報から利用者が選択可能なメニューを生成する技術が記載されている。データベースの保管技術として、文献4に記載されているデータベース内容の改竄検出に必要なデータの保管を、文献5, 6に記載されているデータベースに採用することは、当該技術分野の専門家にとっては自明のものであるし、グループ定義体に対しての変更の際に新たに鍵共有を行う技術は文献3に記載されており当該技術分野の専門家にとっては常套手段である。

請求の範囲: 28-50

文献7: J P, 9-252323, A (ソニー株式会社) 22. 9月. 1997 (22. 09. 979) 第【0028】-【0033】段落,

第【0040】-【0052】段落, 第1-10図

には、広域ネットワークに接続された自組織に属する端末から自組織ネットワーク内のホストに接続する場合、鍵情報とパケットヘッダに含まれる情報から認証情報を作成して当該アクセスの正当性を検証した後、正当な場合のみ該パケットを自組織ネットワークに中継する技術が記載されている。

データベースへのアクセスの可否について、文献6に記載されているデータベースに対して、文献7の外部ネットワークを介した自組織に属する端末からのアクセスの正当性を検証する技術を採用することは、当該技術分野の専門家にとっては自明のものであり、また、送信側にてデータの完全性を認証する技術は、文献4に記載されており、当該技術分野の専門家にとっては常套手段である。

請求の範囲: 51-60

文献1には、メッセージ毎にランダムに発生する鍵を公開鍵暗号により暗号化すると共に、公開鍵証明書や電子署名を付加してデータや送信者の正当性を補償しつつ配送することで、通信当事者間で前記メッセージ毎にランダムに発生する鍵を安全に共有できるプロトコルが記載されている。

文献2には、公開鍵を登録してあるセンタによるセッション鍵の鍵共有プロトコルと、該プロトコルに対する複数の攻撃方法が記載されている。

文献3には、特定グループ内でのメンバー変更に応じてグループ公開鍵を更新し、このグループ公開鍵を用いてグループの各メンバー端末に対して新たな鍵を同報配布する技術が記載されている。

文献4には、情報データと、該情報データを暗号化した署名データと、該署名データの作成に用いた暗号キーの検証データとをデータベースにて保管し、利用者は前記情報データを前記検証データで暗号化した結果を前記署名データと比較することで検証が可能とする技術が記載されている。

各種攻撃に対する鍵の安全な配送、共有を実現するために、文献1に記載されている公開鍵証明書や電子署名を付加してデータや送信者の正当性を補償しつつ文献2, 3に記載されている鍵の配送、共有を行う技術を、文献4に記載されている改竄検出可能な記憶媒体に設けることは、当該技術分野の専門家にとっては自明のものである。

請求の範囲: 61-68

文献4には、情報データと、該情報データを暗号化した署名データと、該署名データの作成に用いた暗号キーの検証データとをデータベースにて保管し、利用者は前記情報データを前記検証データで暗号化した結果を前記署名データと比較することで検証が可能とする技術が記載されている。

文献5には、データベース上の保存情報を参照権限のある複数ユーザで共有する技術が記載されている。

**This Page Blank (uspto)**

補充欄 (いずれかの欄の大きさが足りない場合に使用すること)

第 V. 2 欄の続き

記憶媒体上のデータの更新を行うために、文献4に記載されている改竄検出が可能なデータベースの構造を、文献5に記載されている参照権限のある複数ユーザを対象にしたデータベースに採用することは、当該技術分野の専門家にとっては自明のものであるし、グループ定義体に対しての変更の際に新たに鍵共有を行う技術は文献3に記載されており当該技術分野の専門家にとっては常套手段である。

請求の範囲：69-72, 92-95

文献3には、特定グループ内でのメンバー変更に応じてグループ公開鍵を更新し、このグループ公開鍵を用いてグループの各メンバー端末に対して新たな鍵を同報配布する技術が記載されている。

文献4には、情報データと、該情報データを暗号化した署名データと、該署名データの作成に用いた暗号キーの検証データとをデータベースにて保管し、利用者は前記情報データを前記検証データで暗号化した結果を前記署名データと比較することで検証が可能とする技術が記載されている。

文献6には、データベースにアクセス権限管理ユニットを設け、グループ定義体に基づく利用者帰属情報から利用者が選択可能なメニューを生成する技術が記載されている。

データベースの保管管理技術として、文献3に記載されている鍵共有技術を考慮して、文献4に記載されているデータベース内容の改竄検出に必要なデータの保管を、文献6に記載されているグループ毎のアクセス権限管理を行うデータベースに採用することは、当該技術分野の専門家にとっては自明のものである。

請求の範囲：73-91

文献3には、特定グループ内でのメンバー変更に応じてグループ公開鍵を更新し、このグループ公開鍵を用いてグループの各メンバー端末に対して新たな鍵を同報配布する技術が記載されている。

文献8：JP, 7-245605, A (富士通株式会社)

1995年9月19日 (1995.09.19) 全文, 第1-10図

には、暗号化情報の中継装置に鍵格納部を設け、各加入者に対しては各加入者毎の個別鍵で暗号化して情報を送ることで、メンバーの加入や脱退にも柔軟に対処可能なシステムが記載されている。

文献7には、広域ネットワークに接続された自組織に属する端末から自組織ネットワーク内のホストに接続する場合、鍵情報とパケットヘッダに含まれる情報から認証情報を作成して当該アクセスの正当性を検証した後、正当な場合のみ該パケットを自組織ネットワークに中継する技術が記載されている。

データベースへのアクセスの可否について、文献3に記載されている鍵共有技術を考慮して、文献4に記載されているデータベースに対して、文献8に記載されているの中継技術に文献7の外部ネットワークを介した自組織に属する端末からのアクセスの正当性を検証する技術を採用することは、当該技術分野の専門家にとっては自明のものである。

請求の範囲：96-106

文献4には、情報データと、該情報データを暗号化した署名データと、該署名データの作成に用いた暗号キーの検証データとをデータベースにて保管し、利用者は前記情報データを前記検証データで暗号化した結果を前記署名データと比較することで検証が可能とする技術が記載されている。

文献6には、データベースにアクセス権限管理ユニットを設け、グループ定義体に基づく利用者帰属情報から利用者が選択可能なメニューを生成する技術が記載されている。

データベースの保管技術として、文献4に記載されているデータベース内容の改竄検出に必要なデータの保管を、文献6に記載されているグループ毎のアクセス権限管理

***This Page Blank (uspto)***



補充欄 (いずれかの欄の大きさが足りない場合に使用すること)

第 V. 2 欄の続き

を行うデータベース構成に採用することは、当該技術分野の専門家にとっては自明のものであるし、グループ定義体に対しての変更に際して新たに鍵共有を行う技術は文献3に記載されており当該技術分野の専門家にとっては常套手段である。

*This Page Blank (uspto)*

5640

09701390

PATENT COOPERATION TREATY

## PCT

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

|  |   |   |
|--|---|---|
| Applicant's or agent's file reference<br>KM-90-X   | <b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) |   |
| International application No.<br>PCT/JP99/02973  | International filing date (day/month/year)<br>03 June 1999 (03.06.99)   | Priority date (day/month/year)<br>04 June 1998 (04.06.98) |
| International Patent Classification (IPC) or national classification and IPC<br>C07C 271/10, 271/64, 275/24, 275/50, 333/04, 333/10, C07F 7/10, A01N 47/12, 47/18, 47/24, 47/28, 55/00 |   |   |
| Applicant<br>KUMIAI CHEMICAL INDUSTRY CO., LTD.  |   |   |

|   |
|---|
| 1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.   |
| 2. This REPORT consists of a total of <u>3</u> sheets, including this cover sheet.  |
| <input type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).<br><br>These annexes consist of a total of _____ sheets.   |
| 3. This report contains indications relating to the following items: <ul style="list-style-type: none"> <li>I <input checked="" type="checkbox"/> Basis of the report</li> <li>II <input type="checkbox"/> Priority</li> <li>III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</li> <li>IV <input type="checkbox"/> Lack of unity of invention</li> <li>V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</li> <li>VI <input type="checkbox"/> Certain documents cited</li> <li>VII <input type="checkbox"/> Certain defects in the international application</li> <li>VIII <input type="checkbox"/> Certain observations on the international application</li> </ul> |

|   |  |
|---|--|
| Date of submission of the demand<br>01 December 1999 (01.12.99) | Date of completion of this report<br>15 August 2000 (15.08.2000) |
| Name and mailing address of the IPEA/JP                         | Authorized officer   |
| Facsimile No.   | Telephone No.  |

*This Page Blank (usp...)*

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP99/02973

## I. Basis of the report

## 1. With regard to the elements of the international application:\*

- ☒ the international application as originally filed
- ☐ the description:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the claims:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, as amended (together with any statement under Article 19  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the drawings:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the sequence listing part of the description:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_

## 2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language \_\_\_\_\_ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

## 3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/fig \_\_\_\_\_

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).\*\*

\* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

\*\* Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

This Page Blank (uspto)

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP99/02973

**V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement****1. Statement**

|                               |        |     |     |
|-------------------------------|--------|-----|-----|
| Novelty (N)                   | Claims | 1-9 | YES |
|                               | Claims |     | NO  |
| Inventive step (IS)           | Claims | 1-9 | YES |
|                               | Claims |     | NO  |
| Industrial applicability (IA) | Claims | 1-9 | YES |
|                               | Claims |     | NO  |

**2. Citations and explanations**

None of the documents cited in the international search report or documents found to be relevant describes the phenylacetylene derivatives, agricultural/horticultural bactericides, and method of eliminating agricultural/horticultural bactericide crop damage, and these matters are not obvious to persons skilled in the art.

This Page Blank (uspto)



## PATENT COOPERATION TREATY

PCT

## NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents  
United States Patent and Trademark  
Office  
Box PCT  
Washington, D.C.20231  
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

|  |  |
|--|--|
| Date of mailing (day/month/year)<br>03 February 2000 (03.02.00)      |  |
| International application No.<br>PCT/JP99/02510                      | Applicant's or agent's file reference<br>98P30155        |
| International filing date (day/month/year)<br>14 May 1999 (14.05.99) | Priority date (day/month/year)<br>18 May 1998 (18.05.98) |
| Applicant<br>OHKUBO, Tatsuma et al                                   |  |

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:  
16 December 1999 (16.12.99)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was  
☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

|   |                                     |
|---|-------------------------------------|
| The International Bureau of WIPO<br>34, chemin des Colombettes<br>1211 Geneva 20, Switzerland | Authorized officer<br>Masashi HONDA |
| Facsimile No.: (41-22) 740.14.35  | Telephone No.: (41-22) 338.83.38    |

***This Page Blank (us...)***

09700390

5640  
Translation

PATENT COOPERATION TREATY

PCT

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

|  |   |  |
|--|---|--|
| Applicant's or agent's file reference<br>98P30155  | <b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) |  |
| International application No.<br>PCT/JP99/02510  | International filing date (day/month/year)<br>14 May 1999 (14.05.99)  | Priority date (day/month/year)<br>18 May 1998 (18.05.98) |
| International Patent Classification (IPC) or national classification and IPC<br>H04L 9/08, 9/32, G09C 1/00, G06F 17/30 |   |  |
| Applicant<br>MITSUBISHI MATERIALS CORPORATION  |   |  |

|   |  |
|---|--|
| <p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>5</u> sheets, including this cover sheet.</p> <p><input type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of _____ sheets.</p>   |  |
| <p>3. This report contains indications relating to the following items:</p> <p>I <input checked="" type="checkbox"/> Basis of the report</p> <p>II <input type="checkbox"/> Priority</p> <p>III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p>IV <input type="checkbox"/> Lack of unity of invention</p> <p>V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p>VI <input type="checkbox"/> Certain documents cited</p> <p>VII <input type="checkbox"/> Certain defects in the international application</p> <p>VIII <input type="checkbox"/> Certain observations on the international application</p> |  |

|   |  |
|---|--|
| Date of submission of the demand<br>16 December 1999 (16.12.99) | Date of completion of this report<br>18 August 2000 (18.08.2000) |
| Name and mailing address of the IPEA/JP                         | Authorized officer   |
| Facsimile No.   | Telephone No.  |

*This Page Blank (uspic*

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP99/02510

## I. Basis of the report

## 1. With regard to the elements of the international application:\*

- ☒ the international application as originally filed
- ☐ the description:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the claims:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, as amended (together with any statement under Article 19  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the drawings:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the sequence listing part of the description:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language \_\_\_\_\_ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/fig \_\_\_\_\_

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).\*\*

\* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

\*\* Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

*This Page Blank (uspto)*

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP99/02510

## V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

## 1. Statement

|                               |        |       |     |
|-------------------------------|--------|-------|-----|
| Novelty (N)                   | Claims | 1-106 | YES |
|                               | Claims |       | NO  |
| Inventive step (IS)           | Claims |       | YES |
|                               | Claims | 1-106 | NO  |
| Industrial applicability (IA) | Claims | 1-106 | YES |
|                               | Claims |       | NO  |

## 2. Citations and explanations

## CONCERNING CLAIMS 1-17

Document 1 [Key Distribution, Key Management, and Authentication (MASAHIRO MITSUYASU, EIJI OKAMOTO), bit, Vol. 28, No. 8 (August 1996), pages 87-95] discloses a protocol that enables communicating parties to safely share a key randomly created for each message by encoding a key randomly created for each message using a public key code, and sending while guaranteeing the validity of data with a public key identification or electronic signature or the validity of the sender.

Document 2 [Applied Cryptography, Second Edition, John Wiley & Sons, Inc., (1996), 3.1 Key Exchange, pages 47-52] discloses a key sharing protocol for session keys using a center that registers public keys, and discloses a plurality of methods of attacking that protocol.

Document 3 [JP, 9-212089, A (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.), 15 August 1997 (15.08.97), full text, Figs. 1-12] discloses art that updates a group's public keys in response to changes in members within a specific group and broadcasts new keys to the terminal of each member of the group using this group public key.

Guaranteeing the validity of data with a public key identification or electronic signature or the validity of the sender as described in document 1 while sending and sharing keys as described in documents 2 and 3 in order to implement safe sending and sharing of keys in response to various attacks appears to be obvious to a person skilled in the art of the relevant technical field.

## Concerning Claims 18-27:

Document 4 [JP, 10-13403, A (NEC CORPORATION), 16 January 1998 (16.01.98), full text, Figs. 1-7] discloses art in which information data and signature data encoding that information data and verification data for the code key used in creating that signature data are stored in a database, and a user can verify the aforesaid information data by comparing the result of encoding the aforesaid verification data with the aforesaid signature data.

Document 5 [JP, 7-200617, A (NIPPON TELEGRAPH AND TELEPHONE CORPORATION), 4 August 1995 (04.08.95), full text, Figs. 1-9] discloses art in which information kept in a database is shared by a plurality of users with rights to reference it.

Document 6 [JP, 10-40155, A (FUJITSU LIMITED), 22 February 1998 (13.02.98), paragraphs 0022-0024, paragraphs 0027-0030, Figs. 1-15] discloses art in which a database is provided with an access right control unit, and a user-selectable menu is created from user attribute information based on the group definition body.

Applying the storage of data needed for detecting alterations in database contents as described in document 4 to the databases described in documents 5 and 6 as database storage art appears to be obvious to a person skilled in the art of the relevant technical field. Art that shares new keys when modifying the group definition body is disclosed in document 3 and is a commonly used means for a person skilled in the art of the relevant technical field.

*This Page Blank*



## Supplemental sheet of Box V. 2

## Continuation of Box V. 2

## Concerning Claims 28-50

Document 7 [JP, 9-252323, A (SONY CORPORATION), 22 September 1997 (22.09.1979), paragraphs 0028-0033, paragraphs 0040-0052, Figs. 1-10] discloses art whereby, when connecting to a host within an organization's network from a terminal belonging to the organization connected in a wide-area network, authentication information is created from key information and information included in a packet header, and the validity of that access is verified, after which the packet is relayed to the organization's network only if it is valid.

Applying art for verifying the validity of access from a terminal belonging to an organization via an external network as described in document 7 to the database described in document 6 in order to permit or deny access to the database appears to be obvious to a person skilled in the art of the relevant technical field. Also, art that authenticates the completeness of data at the sending side is disclosed in document 4, and is a commonly used means for a person skilled in the art of the relevant technical field.

## Concerning Claims 51-60

Document 1 discloses a protocol that enables communicating parties to safely share a key randomly created for each message by encoding a key randomly created for each message using a public key code, and sending while guaranteeing the validity of data with a public key identification or electronic signature or the validity of the sender.

Document 2 discloses a key sharing protocol for session keys using a center that registers public keys, and discloses a plurality of methods of attacking that protocol.

Document 3 discloses art that updates a group's public keys in response to changes in members within a specific group and broadcasts new keys to the terminal of each member of the group using this group public key.

Document 4 discloses art in which information data and signature data encoding that information data and verification data for the code key used in creating that signature data are stored in a database, and a user can verify the aforesaid information data by comparing the result of encoding the aforesaid verification data with the aforesaid signature data.

Using art that guarantees the validity of data with a public key identification or electronic signature or the validity of the sender as described in document 1 while sending and sharing keys as described in documents 2 and 3 in order to implement safe sending and sharing of keys in response to various attacks and providing it in a recording medium that can detect alterations as described in document 4 appears to be obvious to a person skilled in the art of the relevant technical field.

## Concerning Claims 61-68

Document 4 discloses art in which information data and signature data encoding that information data and verification data for the code key used in creating that signature data are stored in a database, and a user can verify the aforesaid information data by comparing the result of encoding the aforesaid verification data with the aforesaid signature data.

Document 5 discloses art in which information kept in a database is shared by a plurality of users with rights to reference it.

Applying a database structure that can detect alterations as described in document 4 to a database for a plurality of users with rights to reference it as described in document 5 in order to update data on a recording medium appears to be obvious to a person skilled in the art of the relevant technical field. Art that shares new keys when there are changes in a group definition body is disclosed in document 3 and is a commonly used means for a person skilled in the art of the relevant technical field.

## Concerning Claims 69-72, 92-95

Document 3 discloses art that updates a group's public keys in response to changes in members within a specific group and broadcasts new keys to the terminal of each member of the group using this group public key.

*This Page Blank (uspto)*

## Supplemental sheet of Box V. 2

Continuation of Box V. 2

Document 4 discloses art in which information data and signature data encoding that information data and verification data for the code key used in creating that signature data are stored in a database, and a user can verify the aforesaid information data by comparing the result of encoding the aforesaid verification data with the aforesaid signature data.

Document 6 discloses art in which a database is provided with an access right control unit, and a user-selectable menu is created from user attribute information based on the group definition body.

Referring to key sharing art as described in document 3 and applying storage of data necessary for detecting alterations to database contents as described in document 4 to a database that controls access rights for each group as described in document 6 as database storage control art appears to be obvious to a person skilled in the art of the relevant technical field.

## Concerning Claims 73-91

Document 3 discloses art that updates a group's public keys in response to changes in members within a specific group and broadcasts new keys to the terminal of each member of the group using this group public key.

Document 8 [JP, 7-245605, A (FUJITSU LIMITED), 19 September 1995 (19.09.95), full text, Figs. 1-10] discloses a system that provides an encoded information relay device in a key storage unit; it can flexibly respond to members joining and leaving by sending information encoded by individual keys for each subscriber to each subscriber.

Document 7 discloses art whereby, when connecting to a host within an organization's network from a terminal belonging to the organization connected in a wide-area network, authentication information is created from key information and information included in a packet header, and the validity of that access is verified, after which the packet is relayed to the organization's network only if it is valid.

Referring to key sharing art as described in document 3 and applying art for verifying the validity of access from a terminal belonging to an organization via an external network as described in document 7 to the relay art described in document 8 and to the database described in document 4 in order to permit or deny access to the database appears to be obvious to a person skilled in the art of the relevant technical field.

## Concerning Claims 96-106

Document 4 discloses art in which information data and signature data encoding that information data and verification data for the code key used in creating that signature data are stored in a database, and a user can verify the aforesaid information data by comparing the result of encoding the aforesaid verification data with the aforesaid signature data.

Document 6 discloses art in which a database is provided with an access right control unit, and a user-selectable menu is created from user attribute information based on the group definition body.

Applying storage of data necessary for detecting alterations in database contents as described in document 4 to a database structure that controls access rights for each group as described in document 6 as database storage art appears to be obvious to a person skilled in the art of the relevant technical field. Art that shares new keys when modifying the group definition body is disclosed in document 3 and is a commonly used means for a person skilled in the art of the relevant technical field.

*This Page Blank (usps),*



(法 8 条、法施行規則第40、41条)  
[PCT 18条、PCT規則43、44]

|                             |   |                         |
|-----------------------------|---|-------------------------|
| 出願人又は代理人<br>の書類記号 98P30155  | 今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)<br>及び下記5を参照すること。 |                         |
| 国際出願番号<br>PCT/J P 98/02510  | 国際出願日<br>(日.月.年) 14.05.99                               | 優先日<br>(日.月.年) 18.05.98 |
| 出願人 (氏名又は名称)<br>三菱マテリアル株式会社 |   |                         |

国際調査機関が作成したこの国際調査報告を法施行規則第41条 (PCT 18条) の規定に従い出願人に送付する。  
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 4 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない (第 I 欄参照)。

3. ☐ 発明の単一性が欠如している (第 II 欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☐ 出願人が提出したものを承認する。

☒ 第 III 欄に示されているように、法施行規則第47条 (PCT規則38.2(b)) の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から 1 カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 2 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

This Page Blank (uspto)

## 第Ⅲ欄 要約 (第1ページの5の続き)

チームマスターのデジタル署名、メンバーリスト、共通鍵リストおよび暗号化データを保管する情報保管装置と、メンバー公開鍵を記憶する記憶部と、入力情報の暗号化データを生成する暗号化部と、上記共通鍵を相手方公開鍵にて暗号化し暗号化鍵を生成する暗号化鍵生成部と、上記各暗号化鍵、暗号化データを上記情報保管装置に転送する転送部と、上記情報保管装置からメンバーリストを取得し、該メンバーリストのチームマスターデジタル署名が指定されたデジタル署名と一致するか否かを判断し、一致する場合にのみ上記情報保管装置に変更したリストを転送するリスト管理部と、暗号化鍵情報から共通鍵を復号し、該復号により得た共通鍵で暗号化データを復号する復号化部とを有する暗号化復号化装置とを備えた情報共有システム。

This Page Blank (uspto)



## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.<sup>°</sup> H04L9/08, H04L9/32, G09C1/00, G06F 15/40

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.<sup>°</sup> H04L9/08, H04L9/32, G09C1/00, G06F 15/40

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年  
 日本国公開実用新案公報 1971-1999年  
 日本国登録実用新案公報 1994-1999年  
 日本国実用新案登録公報 1996-1999年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

| 引用文献の<br>カテゴリー* | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示   | 関連する<br>請求の範囲の番号 |
|-----------------|---|------------------|
| Y               | 満保 雅浩, 岡本 栄司, "鍵配送、鍵管理と認証"<br>bit, Vol. 28, No. 8 (8. 1996) 第87-95頁                                       | 1-17, 51-60      |
| Y               | APPLIED CRYPTOGRAPHY SECOND EDITION,<br>"3.1 Key Exchange" (米)<br>John Wiley & Sons, Inc., (1996) 第47-52頁 | 1-17, 51-60      |
| Y               | JP, 10-13403, A (日本電気株式会社)<br>16. 1月. 1998 (16. 01. 98)<br>全文, 第1-7図 (ファミリーなし)                            | 18-106           |

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの  
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
 「O」口頭による開示、使用、展示等に言及する文献  
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献  
 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
 「&」同一パテントファミリー文献

国際調査を完了した日

18. 08. 99

国際調査報告の発送日

31.08.99

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)  
 郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5W

4229

電話番号 03-3581-1101 内線 3576

This Page Blank (uspto)

| C (続き) . 関連すると認められる文献 |   |                  |
|-----------------------|---|------------------|
| 引用文献の<br>カテゴリー*       | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示   | 関連する<br>請求の範囲の番号 |
| Y                     | JP, 7-200617, A (日本電信電話株式会社)<br>4. 8月. 1995 (04. 08. 95)<br>全文, 第1-9図 (ファミリーなし)   | 18-27, 61-68     |
| Y                     | JP, 10-40155, A (富士通株式会社)<br>13. 2月. 1998 (13. 02. 98)<br>第 [0022] - [0024] 段落, 第 [0027] - [0030] 段落,<br>第1-15図 (ファミリーなし) | 18-60, 96-106    |
| Y                     | JP, 7-245605, A (富士通株式会社)<br>19. 9月. 1995 (19. 09. 95)<br>全文, 第1-10図<br>& GB, 2287160, A & US, 5642420, A                 | 73-91            |
| Y                     | JP, 9-252323, A (ソニー株式会社)<br>22. 9月. 1997 (22. 09. 97)<br>第 [0028] - [0033] 段落, 第 [0040] - [0052] 段落,<br>第1-10図 (ファミリーなし) | 28-50, 78-91     |

This Page Blank (uspto)

特許協力条約に基づいて公開された国際出願

**(57) Abstract**  
An information sharing system comprising an information holding device for holding the digital signature of a team master, a member list, a common key list, and encrypted data, and an encrypting/decoding device provided with a storage unit for storing a member public key, an encrypting unit for generating encrypted data on inputted information, an encrypted key creating unit for encrypting the common key by means of the other-party public key and creating an encrypted key, a transfer unit for transferring the encrypted key and encrypted data to the information holding device, a list managing unit for acquiring the member list from the information holding device, judging whether or not the team master's digital signature of the member list agrees with a specified digital signature, and transferring the changed list to the information holding device only when the team master's digital signature agrees with the specified digital signature, and a decoding unit for restoring the common key from the encrypted key information and decoding the encrypted data by means of the common key obtained by the decoding.

## (57)要約

本発明は、情報共有システムに関する。

本発明は、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能な情報共有システムであって、少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能な情報保管装置と、情報を見てもよい少なくとも一のメンバーの公開鍵を記憶する記憶部と、情報を暗号化するための共通鍵を用いる上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する暗号化部と、暗号化に用いた共通鍵を、上記記憶部に記憶され指定された公開鍵で暗号化し、暗号化鍵を生成する暗号化鍵生成部と、上記複数の暗号化鍵および暗号化データを上記情報保管装置に転送する転送部と、上記情報保管装置からメンバーリストを取得して、当該メンバーリストのチームマスターのデジタル署名が指定されたデジタル署名と一致するか否かを判断し、一致する場合にのみ追加するメンバーの公開鍵の登録または脱会するメンバーの公開鍵の削除を行い、追加登録または削除の場合、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含む新メンバーリストを作成して上記情報保管装置に転送するリスト管理部と、上記情報保管装置から所望の暗号化鍵情報および暗号化データを取得して、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で取得した暗号化データを復号する復号化部とを有する暗号化復号化装置とを備えた情報共有システムである。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE アラブ首長国連邦  
AL アルバニア  
AM アルメニア  
AT オーストリア  
AU オーストラリア  
AZ アゼルバイジャン  
BA ボスニア・ヘルツェゴビナ  
BB バルバドス  
BE ベルギー  
BF ブルキナ・ファソ  
BG ブルガリア  
BJ ベナン  
BR ブラジル  
BY ベラルーシ  
CA カナダ  
CF 中央アフリカ  
CG コンゴ  
CH スイス  
CI コートジボアール  
CM カメルーン  
CN 中国  
CR コスタ・リカ  
CU キューバ  
CY キプロス  
CZ チェッコ  
DE ドイツ  
DK デンマーク

DM ドミニカ  
EE エストニア  
ES スペイン  
FI フィンランド  
FR フランス  
GA ガボン  
GB 英国  
GD グレナダ  
GE グルジア  
GH ガーナ  
GM ガンビア  
GN ギニア  
GW ギニア・ビサウ  
HR クロアチア  
HU ハンガリー  
ID インドネシア  
IE アイルランド  
IL イスラエル  
IN インド  
IS アイスランド  
IT イタリア  
JP 日本  
KE ケニア  
KG キルギスタン  
KP 北朝鮮  
KR 韓国

KZ カザフスタン  
LC セントルシア  
LI リヒテンシュタイン  
LK スリ・ランカ  
LR リベリア  
LS レソト  
LT リトアニア  
LU ルクセンブルグ  
LV ラトヴィア  
MA モロッコ  
MC モナコ  
MD モルドヴァ  
MG マダガスカル  
MK マケドニア旧ユーゴスラヴィア  
共和国  
ML マリ  
MN モンゴル  
MR モーリタニア  
MW マラウイ  
MX メキシコ  
NE ニジェール  
NL オランダ  
NO ノルウェー  
NZ ニュージーランド  
PL ポーランド  
PT ポルトガル  
RO ルーマニア

RU ロシア  
SD スーダン  
SE スウェーデン  
SG シンガポール  
SI スロベニア  
SK スロヴァキア  
SL シエラレオネ  
SN セネガル  
SZ スワジランド  
TD チャード  
TG トーゴ  
TJ タジキスタン  
TZ タンザニア  
TM トルクメニスタン  
TR トルコ  
TT トリニダード・トバゴ  
UG ウグランド  
UA ウクライナ  
US 米国  
UZ ウズベキスタン  
VN ヴェトナム  
YU ユーゴスラビア  
ZA 南アフリカ共和国  
ZW ジンバブエ

## 明細書

情報共有システム

### 技術分野

本発明は、複数のユーザ間での情報共有を目的とし、情報の覗き見や改竄を防ぐための情報共有システムおよびその情報処理方法、並びに記録媒体に関するものである。

### 背景技術

近年のコンピュータ・ネットワーク技術の発展に伴い、様々なデジタル情報がコンピュータネットワーク上で利用されるようになった。

しかし、これらのデジタル情報は、コンピュータ上や、ネットワーク上では、他人の覗き見や改竄が容易である。

そこで、特に秘匿の必要があるユーザのプライベート情報やビジネス情報などは、暗号化技術を利用して暗号化した後、取得、伝達、加工、記録する必要がある。

このような秘匿する必要のある情報を暗号化するために、データ暗号規格（DES：Data Encryption Standard）などの共通鍵暗号方式が開発された。

この方式では、データを暗号化する暗号鍵をユーザ間で共有するため、他のユーザに暗号鍵が取得されないように、配送、記録する必要があった。

そのため、この暗号鍵を覗き見や改竄、取得されないようにするために、暗号鍵を別の鍵でさらに暗号化した状態の鍵である暗号化鍵として配送する部が提案されている。

ある情報を共有したい複数のユーザがいる場合に、上記の手法で情報を暗号化するには、これらの暗号鍵や暗号鍵を暗号化するための鍵を管理す

る鍵管理システムや、情報を共有するユーザをグループ化して管理するグループ管理サーバ、情報へのアクセス制御部などを利用する必要がある。

このように特定グループで秘匿データを共有する場合の共通鍵管理は、サーバで行われ、このサーバにはサーバ管理者が設けられる。

ところが、このサーバ管理者が当該特定グループに含まれない場合には、何の障害もなくデータを覗くことができることになる。

また、サーバ管理者が当該特定グループに含まれたとしても、一存でグループメンバーを変更することができ、データの管理上、万全であるとはいえない。

#### 発明の開示

それゆえ、本発明の目的の一は、暗号化情報を保管するデータベースや、サーバ、ファイルシステム等の管理者による情報の内容の覗き見や改ざんを防止できる情報共有システムおよびその情報処理方法、並びに記録媒体を提供することにある。

当該発明によれば、その目的は、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能な情報共有システムであって、少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能な情報保管装置と、情報を見てもよい少なくとも一のメンバーの公開鍵を記憶する記憶部と、情報を暗号化するための共通鍵を用いる上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する暗号化部と、暗号化に用いた共通鍵を、上記記憶部に記憶され指定された公開鍵で暗号化し、暗号化鍵を生成する暗号化鍵生成部と、上記複数の暗号化鍵および暗号化データを上記情報保管装置に転送する転送部と、上記情報保管装置



からメンバーリストを取得して、当該メンバーリストのチームマスターのデジタル署名が指定されたデジタル署名と一致するか否かを判断し、一致する場合にのみ追加するメンバーの公開鍵の登録または脱会するメンバーの公開鍵の削除を行い、追加登録または削除の場合、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含む新メンバーリストを作成して上記情報保管装置に転送するリスト管理部と、上記情報保管装置から所望の暗号化鍵情報および暗号化データを取得して、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で取得した暗号化データを復号する復号化部とを有する暗号化復号化装置とを備えた情報共有システムという装置により達せられる。

当該発明によれば、グループで共有鍵を共有することができ、暗号化データを保管するデータベースや、サーバ、ファイルシステムの管理者に情報の内容を見られてしまう可能性もない。

また、当該発明によれば、その目的は、送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成部と、前記受信内容確認情報を前記ネットワークを介して送信する送信部と、前記ネットワークを介して前記受信内容確認情報を受信する受信部と、前記送信者側端末から送信される前記情報と前記受信内容確認情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知部とを具備する情報改竄検知装置という装置により達せられる。

当該発明によれば、発明によれば、受信内容確認情報、送信内容確認情

報を用いて改竄検知を行うように構成したので、受信した情報を復号化する権利を有しない端末であっても、情報の改竄を検知することができる。

また、当該発明によれば、その目的は、鍵暗号化部と、暗号化部とからなる暗号化装置において、前記鍵暗号化部は、共通鍵暗号方式を利用して暗号化に用いる共通鍵を取得または生成する共通鍵取得部と、公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化鍵とする共通鍵暗号化部と、前記共通鍵より共通鍵改竄検出に利用する鍵情報を作成する第1共通鍵改竄検出情報作成部とからなり、前記暗号化部は、前記共通鍵を用いて平文を暗号化し暗号文とするデータ暗号化部と、前記平文より第1データ改竄検出情報を作成する第1データ改竄検出情報作成部とからなる暗号化装置という装置により達せられる。

当該発明によれば平文毎に改竄検出情報を作成することはせず、各平文を暗号化する共通鍵に対して改竄検出情報となる鍵情報を作成し、改竄検出と共通鍵作成者の本人確認を可能としたので、情報を暗号化した暗号化情報のオーバーヘッドを減少させることができる。したがって、暗号化情報の転送時におけるネットワークにかかる負荷と暗号化情報を保管する際に要する記憶装置の容量を減少させることができる。

また、当該発明によれば、その目的は、チームを階層化するためのチームデータリストを管理するチームデータリスト管理装置であって、所定の要求先に前記チームデータリストの操作要求を行い、該操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理者のデジタル署名を含むオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チ

ームの管理者のデジタル署名を含むオーソリティリストを有するチームデータリストを前記要求先から取得し、前記識別子を用いて取得されたチームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストのデジタル署名が改竄されていないこと及び前記管理者情報を用いて権限を持つ者によるデジタル署名であることを確認して、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認部と、該正当性確認部によって正当性が確認された前記チームデータリストに対して前記操作要求に応じた変更を加えるチームデータリスト変更部と、前記操作要求を行った指示者のデジタル署名を作成し、前記変更されたチームデータリストに該デジタル署名を添付して前記要求先に送出するデジタル署名部とを具備するチームデータリスト管理装置という装置により達せられる。

当該発明によれば、オーソリティリストとオーソリティデータの含まれたチームデータリストを用いることで各チームの下にサブチームを作成することができ、階層化されたチームを構築することができる。

また、当該発明によれば、その目的は、送信する情報を暗号化した暗号化情報を含む暗号情報を作成する暗号情報作成装置と、同報通信の被配信メンバーの公開鍵が含まれるメンバーリストを管理するメンバーリスト管理装置と、前記暗号化情報を復号化する暗号情報復号化装置と、前記暗号情報作成装置より送信された暗号情報を受信し、該暗号情報を前記メンバーリストをもとに1以上の前記暗号情報復号化装置に配信する情報中継装置と、からなる同報通信システムにおけるメンバーリスト管理装置であって、同報通信を行う1以上のメンバーの公開鍵を含むメンバーリストを作成するリスト作成部と、前記公開鍵を取得し保存する公開鍵管理部とを備えるメンバーリスト管理装置という装置により達せられる。

当該発明によれば、情報中継装置において暗号化された情報を復号化し

ない仕組みとしたので、情報中継装置の管理者による同報通信の通信内容の漏洩や改竄等の不正を防ぎ、本当に情報を共有する必要があるメンバーにだけ同報通信内容を共有することができる。

また、当該発明によれば、その目的は、変更指示を行う指示者の本人識別・認証を行うための情報を所定の要求先に通知して、資源を互いに共有するメンバで構成されるチームに関わる情報と該情報の管理権限を有するマスタのデジタル署名とが含まれ、チームに属するメンバの権限に応じて用意されたチームデータリストを前記要求先から取得し、取得された該チームデータリストの内容に基づいて、権限を持つマスタが前記チームデータリストを作成したか否かを確認するリスト作成者確認部と、該権限を持つマスタの作成であることが確認された前記チームデータリストに対して前記変更指示に応じた変更を加えるリスト変更部と、前記指示者のデジタル署名を作成し、前記リスト変更部で変更されたチームデータリストに該デジタル署名を添付して前記要求先に送るデジタル署名部とを具備するチームデータリスト管理装置という装置により達せられる。

当該発明によれば、正当な権限を持つマスタからの変更指示に応じて、サーバ等に保管されているマスタリスト及びメンバリスト等のチームデータリストを取得し、これらリストが権限を持つマスタによって正当に作成されたことを確認した後に、これらリストに変更を加えて要求先へ返すようにしている。こうしたことから、マスタ以外の一般のメンバ、サーバの管理者、クラッカ等の正当な権限を持たない者がチームデータリストを不正に操作したことを検知できる。

#### 図面の簡単な説明

図 1 は、第 1 の実施形態の発明に係る情報共有システムの基本的な構成

図である。

図 2 は、第 1 の実施形態の発明に係る暗号化復号化装置の構成例を示すブロック図である。

図 3 は、図 2 の復号化部の構成例を示す図である。

図 4 は、WWWサーバの保管される各種リストを示す図である。

図 5 は、第 1 の実施形態の発明に係る情報管理装置としてのWWWサーバにおけるDBMSの詳細な機能を説明するための図である。

図 6 は、グループで共通鍵を共有する場合であって、グループへの公開鍵IDの登録動作例を説明するための図である。

図 7 は、グループで共通鍵を共有する場合であって、共通鍵の登録動作例を説明するための図である。

図 8 は、グループで共通鍵を共有する場合であって、データを暗号化する場合の動作例を説明するための図である。

図 9 は、共有したいユーザを別途してする場合であって、データを暗号化する場合動作例を説明するための図である。

図 10 は、復号化動作例を説明するための図である。

図 11 は、第 2 の実施形態の発明の一実施形態による情報改竄検知装置の動作原理を説明するブロック図である。

図 12 は、同一実施形態による情報改竄検知装置の構成を示すブロック図である。

図 13 は、図 12 に示す受信内容確認情報確認部 103β の動作を説明するフローチャートである。

図 14 は、図 12 に示す送信内容確認情報作成部 104β の動作を説明するフローチャートである。

図 15 は、図 12 に示す受信内容確認情報作成部 202β の動作を説明するフローチャートである。

図 1 6 は、図 1 2 に示す送信内容確認情報確認部 2 0 5  $\beta$  の動作を説明するフローチャートである。

図 1 7 は、従来の情報改竄検知装置の動作原理を説明する図である。

図 1 8 は、従来の情報改竄検知装置の欠点を説明する図である。

図 1 9 は、第 3 - 1 ~ 第 3 - 3 の実施形態の発明の一実施形態である暗号化復号化装置の構成を示すブロック図である。

図 2 0 は、第 3 - 1 ~ 第 3 - 3 の実施形態の発明の一利用形態を示す図である。

図 2 1 は、暗号化に係る動作を説明するフローチャートである。

図 2 2 は、暗号化前の情報と暗号化情報の構成を示す図である。

図 2 3 は、復号化に係る動作を説明するフローチャートである。

図 2 4 は、暗号化情報に情報を追加する際の動作を説明するフローチャートである。

図 2 5 は、暗号化情報に情報を追加する前後の暗号化情報の構成を示す図である。

図 2 6 は、共有メンバー B が、チームに共有メンバー C を追加する際の動作を説明するフローチャートである。

図 2 7 は、チームに共有メンバー C を追加する前後の暗号化情報の構成を示す図である。

図 2 8 は、チームから共有メンバーを削除する際の動作を説明するフローチャートである。

図 2 9 は、チームから共有メンバー A を削除する前後の暗号化情報の構成を示す図である。

図 3 0 は、第 3 - 1 の実施例における情報保管装置に記憶されている情報を示す図である。

図 3 1 は、第 3 - 2 の実施例において情報を追加した際の情報保管装置

に記憶されている情報を示す図である。

図32は、第3-3の実施例において復号化後のスケジュールの表示例を示す図である。

図33は、従来の暗号化・デジタル署名方式における暗号化の動作を説明するフローチャートである。

図34は、従来の暗号化・デジタル署名方式における復号化の動作を説明するフローチャートである。

図35は、特開平8-156964に開示されている暗号化方式による暗号化前の情報と暗号化情報の構成を示す図である。

図36は、特開平9-71388に開示されている暗号化方式による暗号化前の情報と暗号化情報の構成を示す図である。

図37は、第4-1実施形態によるチームデータリスト管理装置及びチームデータリスト保管装置を有するシステムの構成を示したブロック図である。

図38A、B、C、Dは、第4-1実施形態において、チームデータリスト保管装置が設置されたサーバ側に記憶されるチームデータリストの構造を示した説明図である。

図39は、第4-1実施形態におけるチームの階層の一例を示した説明図である。

図40は、図39に示すチーム階層の各チームについてチームデータリストの具体的な値を記入した説明図である。

図41は、第4-1実施形態においてサブチームを作成するための処理手順を示した説明図である。

図において(A)は、メンバCによるサブチーム作成要求(チーム101の下に、チームマスタをXとして、サブチーム103 $\delta$ を作成)を意味し、S11 $\delta$ ~S15 $\delta$ の意味するところは、各々次の通りである。

S11 $\delta$ : サブチーム作成要求

S12 $\delta$ : データリスト管理装置30 $\delta$ は、チーム101 $\delta$ に関する情報(他の101 $\delta$ のサブチームの情報などを含む)を取得

S13 $\delta$ : AUD $\delta$ 、AUL $\delta$ を作成

S14 $\delta$ : 新規に作成した103 $\delta$ のAUD $\delta$ 、AUL $\delta$ を転送(103 $\delta$ のAUD $\delta$ 、AUL $\delta$ 保存要求)

S15 $\delta$ : チーム101 $\delta$ のAUD $\delta$ とAUL $\delta$ を調べる。Cは、サブチーム作成権限者に選ばれているので、正当な権限を持

9/1

つものによる作成要求と判断し、103δのAUDδとAULδを保管

また図において(B)は、メンバXによるチーム103δの管理要求を意味し、S16δ~S19δの意味するところは、各々次の通りである。

S16δ: チーム103δのリスト要求

S17δ: チーム101δ、103δのAUDδとAULδを転送

S18δ: 2つのリストは、親チーム101δのチームマスタによって指名されたCによって、チーム103δが作成されているので、Xは、そのリストが正常な状態で取得していることがわかる

S19δ: Xは、チーム101δのオーソリティリストを作成

また図において(C)は、メンバXによるサブチーム作成権限者(subAUδ)としてのWとVの指定を意味し、S20δ~S21δの意味するところは、各々次の通りである。

S20δ: 更新された103δのAUDδとAULδを転送(103δのAUDδ、AULδ保存更新要求)

S21δ: サーバSV側に保管されているリストにより、Xが間違いなく、Aによる管理体系の中で正当に103δのチームマスタとして任命されていることを検証できる

図42は、図41の処理過程でサブチーム作成要求時に行われるサーバ側の権限確認機能についてその処理手順を示した説明図である。

図43は、図41の処理過程で実施されるクライアント側のリスト正当



## 10

正当性検証に関わる処理手順を示した説明図である。

図44は、図41の処理過程において、クライアント側で新規に作成したチームデータリストをサーバ側で権限確認を行う際の処理手順を示す説明図である。

図45は、第4-1実施形態において、サブチームのチームマスタを変更するための処理手順を示した説明図である。

図46は、第4-1実施形態において、サブオーソリティの作成権限を変更（削除）するための処理手順を示した説明図である。

図47は、第4-1実施形態において、サブチームを削除するための処理手順を示した説明図である。

図において（A）は、メンバCによる以前作成した101 $\delta$ のサブチーム103 $\delta$ の削除を意味し、S81 $\delta$ ～S82 $\delta$ の意味するところは、各々次の通りである。

S81 $\delta$ ：命令を転送

S82 $\delta$ ：チーム101 $\delta$ 、103 $\delta$ のAUD $\delta$ 、AUL $\delta$ を見ると、  
101 $\delta$ のsubAUであるCが103 $\delta$ を作成している  
（103 $\delta$ のAUD $\delta$ に署名している）ことがわかるので  
正当な権限で発行された削除命令と判断して、103 $\delta$ の  
AUD $\delta$ とAUL $\delta$ を削除する

また図において（B）は、メンバAの権限によるチーム103 $\delta$ の削除要求を意味し、S83 $\delta$ ～S84 $\delta$ の意味するところは、各々次の通りである。

S83 $\delta$ ：命令を転送

S84 $\delta$ ：チーム101 $\delta$ 、103 $\delta$ のAUD $\delta$ 、AUL $\delta$ を見ると、  
101 $\delta$ のTM $\delta$ であるAがsubAUとして指名したC  
が103 $\delta$ を作成している（103 $\delta$ のAUD $\delta$ に署名し  
ている）ことがわかるので、正当な権限で発行された削除  
命令と判断して、103 $\delta$ のAUD $\delta$ とAUL $\delta$ を削除す  
る

図48は、クライアント側に居るユーザの権限確認を行う際にサーバが用いるシェイクハンドないしチャレンジレスポンスと呼ばれる手法の手順を示した説明図である。

図49は、第4-2実施形態におけるチームの階層の一例を示した説明図である。

図50は、第4-3実施形態におけるチームの階層の一例を示した説明図である。

図51は、アクセス制御リストを利用して情報共有を行う従来のシステムの構成

10/1

を示したブロック図である。

図52は、第5の実施形態の発明の同報通信システムの仕組みを示す図である。

図53は、一般的なメンバーリストの例である。

図54は、複数のリストで構成されたメンバーリストの一例である。

図55は、本発明のメンバーリスト管理装置の実施の形態を示す図である。

図56は、リスト作成部の動作フローチャートである。

図 5 7 は、第 5 の実施形態の発明の暗号情報作成装置の実施の形態を示す図である。

図 5 8 は、第 5 の実施形態の発明の同報通信システムにおける暗号化復号化過程を示す図である。

図 5 9 は、第 5 の実施形態の発明の同報通信システムにおける複数パース送信および複数パース受信の仕組みを説明する図である。

図 6 0 は、第 5 の実施形態の発明の暗号情報復号化装置の実施の形態を示す図である。

図 6 1 は、第 5 の実施形態の発明の情報中継装置の実施の形態を示す図である。

図 6 2 は、第 5 の実施形態の発明の同報通信システムを証券ニュース配信システムとして応用した実施例である。

図 6 3 は、メーリングリストサーバを利用した本発明の同報通信システムの 1 実施例である。

図 6 4 は、従来の同報通信システムの仕組みを説明する図である。

図 6 5 は、特開平 7 - 2 4 5 6 0 5 に開示されている同報通信システムの仕組みを説明する図である。

図 6 6 は、第 6 の実施形態の発明の一実施形態によるチームデータリスト管理装置及びチームデータリスト保管装置を有するシステムの構成を示したブロック図である。

図 6 7 は、第 6 の実施形態の発明の前提となる技術を説明するための第 1 の図であって、メンバリストの管理機能及び保管機能をクライアントーサーバ間で分割した構成を示したブロック図である。

図 6 8 は、第 6 の実施形態の発明の前提となる技術を説明するための第 2 の図であって、クライアント側からサーバ上のメンバリストに含まれているメンバ変更を行う場合の処理手順について示した説明図である。

## 1 2

図6 9は、クライアント側に居るユーザの権限確認を行う際にサーバが用いるシェイクハンドないしチャレンジレスポンスと呼ばれる手法の手順を示した説明図である。

図7 0は、上記実施形態において、複数の管理者によってメンバを管理する場合のメンバ変更に関する処理手順を示した説明図である。

図7 1は、同実施形態において、クライアント側で行われるリスト作成者確認の処理手順を示したフローチャートである。

図7 2は、同実施形態において、複数の管理者によってメンバを管理する場合のサブマスタ変更に関する処理手順を示した説明図である。

図7 3は、同実施形態において、複数の管理者によってメンバを管理する場合のチームマスタ変更に関する処理手順を示した説明図である。

図7 4は、同実施形態において、図7 3に示すチームマスタ変更時にサーバ側で行われる権限確認の処理手順を示したフローチャートである。

図においてS 6 1と～S 6 5との意味するところは、各々次の通りである。

S 6 1と：新・旧チームマスタリスト、新メンバリストの取得

S 6 2と：2つのリストのデジタル署名確認：改竄されていないか？

（このときS 6 2と（NO）＝クライアントからサーバ側へ転送中に不正行為（改竄等）が発生したため、処理中止）

S 6 3と：新チームマスタリストは、旧チームマスタリストのチームマスタによるデジタル署名となっているか？

（このときS 6 3と（NO）＝不正行為（改竄等）が発生したため、処理中止）

S 6 4と：新チームマスタリストのデジタル署名者は、マスタ権限を持っているか？

（このときS 6 4と（NO）＝この時点で、チームマスタ自身の変更時と判断できる。またS 6 4と（YES）＝通常の変更。ただし、管理者自身の変更ではない）

S 6 5と：新メンバリストのデジタル署名者は、①新チームのマスタリストに含まれているか？もしくは②旧（新）チームマスタリストのデジタル署名者であるか？

（このときS 6 5と（YES）＝正当な権限を持つチームマスタによって正常な操作でチームマスタ自身を変更したと判断する。またS

12/1

64と（NO）＝不正行為（改竄等）が発生したため、処理中止）

図75は、同実施形態において、図74に示す権限確認を行う場合に同図の各ステップで比較照合されるチームマスタリスト及びメンバリストの様子を示した説明図である。

図76は、アクセス制御リストを利用して情報共有を行う従来のシステムの構成を示したブロック図である。

図77は、特定グループに属するメンバだけで情報を共有するためにクライアントーサーバ間で行われる処理手順を示した説明図である。

#### 発明を実施するための最良の形態

以下の実施例はクレームにかかる発明を限定するものではない。また、目的の達成のために、実施例中で説明されている特徴のすべての組み合わせが必ずしも必要となるものではない。

[第 1 の実施形態]

第 1 の実施形態の発明は、複数のユーザ間での情報共有を目的とし、情報の覗き見や改竄を防ぐための情報共有システムおよびその情報処理方法、並びに記録媒体に関するものである。

第 1 の実施形態の発明に関し、従来以下説明する技術が知られている。

近年のコンピュータ・ネットワーク技術の発展に伴い、様々なデジタル情報がコンピュータネットワーク上で利用されるようになった。

しかし、これらのデジタル情報は、コンピュータ上や、ネットワーク上では、他人の覗き見や改竄が容易である。

そこで、特に秘匿の必要があるユーザのプライベート情報やビジネス情報などは、暗号化技術を利用して暗号化した後、取得、伝達、加工、記録する必要がある。

このような秘匿する必要のある情報を暗号化するために、データ暗号規格（DES : Data Encryption Standard）などの共通鍵暗号方式が開発された。

この方式では、データを暗号化する暗号鍵をユーザ間で共有するため、他のユーザに暗号鍵が取得されないように、配送、記録する必要があった。

そのため、この暗号鍵を覗き見や改竄、取得されないようにするために、暗号鍵を別の鍵でさらに暗号化した状態の鍵である暗号化鍵として配送する方法が提案されている。

ある情報を共有したい複数のユーザがいる場合に、上記の手法で情報を暗号化するには、これらの暗号鍵や暗号鍵を暗号化するための鍵を管理する鍵管理システムや、情報を共有するユーザをグループ化して管理するグ

ループ管理サーバ、情報へのアクセス制御部などを利用する必要がある。

このように特定グループで秘匿データを共有する場合の共通鍵管理は、サーバで行われ、このサーバにはサーバ管理者が設けられる。

ところが、このサーバ管理者が当該特定グループに含まれない場合には、何の障害もなくデータを覗くことができることになる。

また、サーバ管理者が当該特定グループに含まれたとしても、一存でグループメンバーを変更することができ、データの管理上、万全であるとはいえない。

本発明は、かかる事情に鑑みてなされたものであり、その目的は、暗号化情報を保管するデータベースや、サーバ、ファイルシステム等の管理者による情報の内容の覗き見や改ざんを防止できる情報共有システムおよびその情報処理方法、並びに記録媒体を提供することにある。

第1の実施形態の発明によれば、複数ユーザが共有したい情報を秘匿しておくために、たとえば共有鍵暗号方式と公開鍵暗号方式が併用される。入力情報は、共有鍵暗号方式で、共通鍵を用いて暗号化される。

また、本発明によれば、たとえばネットワーク上での情報共有システムが実現される。

このシステムでは、少なくとも複数のメンバーでアクセス可能な情報保管装置に、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管される。

グループに属するメンバーを追加登録する場合、情報保管装置からメンバーリストが取得され、取得したメンバーリストのチームマスターのデジタル署名が指定されたデジタル署名と一致するか否かを判断される。

そして、一致する場合にのみ、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含む新メンバーリストが作成され、作成されたメンバーリストが情報保管装置に転送され保管される。

また、グループに属するメンバーで利用する共通鍵を登録する場合、情報保管装置からメンバーリストが取得され、取得したメンバーリストのチームマスターのデジタル署名が指定されたデジタル署名と一致するか否かを判断される。

そして、一致する場合にのみ、指定されている公開鍵を用いて登録すべき共通鍵が暗号化され、暗号化された共通鍵が情報保管装置に転送され保管される。

また、共通鍵を用いてデータを暗号化する場合、情報保管装置の共通鍵リストから少なくとも暗号化鍵情報が取得され、この暗号化鍵情報から共通鍵が復号される。

そして、復号した共通鍵で共通鍵暗号化方式に基づいて入力情報が暗号化されて暗号化データが生成され、暗号化されたデータが情報保管装置に転送され保管される。

また、データを復号する場合には、情報保管装置から所望の暗号化鍵情報および暗号化データが取得され、この暗号化鍵情報から共通鍵が復号されり。

そして、復号した共通鍵で取得した暗号化データが復号される。



また、情報保管装置では、メンバーリスト変更要求があると、グループ管理手段により要求に応じたメンバーリストの変更が行われる。

また、共通鍵の登録要求があると、共通鍵管理部により、要求のあった共通鍵がその暗号化鍵情報を含めて登録される。また、共通鍵の取得要求があると、共通鍵管理部により、特定グループでの情報共有に最適な共通鍵が選択されて、要求先に転送される。

また、暗号化データの登録要求があると、暗号化データ管理部により、暗号化データが当該データの暗号化に用いられた共通鍵情報とともに保管される。また、暗号化データの取得要求があると、暗号化データ管理部により、保管暗号化データおよび共通鍵情報が要求先に転送される。

以下、第 1 の実施形態を図面に関連付けて詳細に説明する。

図 1 は本発明に係る情報共有システムの基本的な構成図、図 2 は本発明に係る暗号化復号化装置の構成例を示すブロック図である。

本実施形態（第 1 の実施形態）に係る情報共有システムは、図 1 に示すように、図 2 に示す暗号化復号化装置 10α が組み込まれた第 1 の端末装置 1 および第 2 の端末装置 2α、並びに暗号化復号化装置 10α で生成されたメンバーリストや、共通鍵リスト、暗号化データ等を保管するための情報保管装置としての WWW サーバ 3α が、ネットワーク（たとえば、インターネット）4α で接続されて構成されている。

暗号化復号化装置 10α は、暗号化部 11α、共通鍵生成部 12α、記憶部 13α、暗号化鍵生成部 14α、付加情報生成部 15α、転送部 16α、デジタル署名確認部 17α、公開鍵管理部 18α、デジタル署名付加

部 1 9  $\alpha$ 、並びに復号化部 2 0  $\alpha$ により構成されている。

そして、デジタル署名確認部 1 7  $\alpha$ 、公開鍵管理部 1 8  $\alpha$ 、およびデジタル署名付加部 1 9  $\alpha$ を主要素としてリスト管理部が構成される。

暗号化部 1 1  $\alpha$ は、情報を暗号化するための共通鍵  $d k \alpha$ またはWWWサーバ 3  $\alpha$ から読み出した共通鍵  $c k \alpha$ を用いて、たとえば共有鍵暗号方式（たとえばDES）により入力情報  $M \alpha$ を暗号化して暗号化データ  $M' \alpha$ を生成し、生成した暗号化データ  $M' \alpha$ を転送部 1 6  $\alpha$ に出力する。

また、暗号化部 1 1  $\alpha$ は、グループで共通鍵を共有する場合であって、データを暗号化する場合に、特定グループのメンバーリスト要求、具体的にはグループIDやユーザ公開鍵IDを含むメンバーリスト要求をWWWサーバ 3  $\alpha$ に対して行う。この要求の転送は転送部 1 6  $\alpha$ を介して行われる。

共通鍵生成部 1 2  $\alpha$ は、たとえば乱数発生回路等により構成され、情報を暗号化するための共通鍵  $d k \alpha$ を生成し、暗号化部 1 1  $\alpha$ および暗号化鍵生成部 1 4  $\alpha$ に出力する。なお、共通鍵  $d k \alpha$ は、たとえば64ビットデータとして生成される。

記憶部 1 3  $\alpha$ は、たとえばハードディスクにより構成され、本システムを共有する複数  $n$ のユーザ各々の固有の公開鍵  $P K 1 \alpha$ 、 $P K 2 \alpha$ 、 $\dots$ 、 $P K n \alpha$ があらかじめ記録されており、暗号化鍵生成部 1 4  $\alpha$ および公開鍵管理部 1 8  $\alpha$ によりアクセスされる。

暗号化鍵生成部 1 4  $\alpha$ は、暗号化に用いた共通鍵  $d k \alpha$ （または共通鍵  $c k \alpha$ ）を、記憶部 1 3  $\alpha$ に記録されているユーザの公開鍵を用い、たと

例えば公開鍵暗号方式（たとえばRSA）に基づいて暗号化し、1または複数の暗号化鍵 $E K 1 \alpha$ ,  $E K 2 \alpha$ , ...,  $E K n \alpha$ を生成し、生成した暗号化鍵 $E K 1 \alpha$ ,  $E K 2 \alpha$ , ...,  $E K n \alpha$ を転送部16 $\alpha$ に出力する。

また、暗号化鍵生成部14 $\alpha$ は、特定グループに属するメンバーだけで情報を共有したい場合であって、そのメンバーで利用する共通鍵の登録を行う場合、特定グループのメンバーリスト要求をWWWサーバ3 $\alpha$ に対して行う。この要求の転送は転送部16 $\alpha$ を介して行われる。

付加情報生成部15 $\alpha$ は、たとえば共通鍵 $d k \alpha$ のメッセージダイジェスト $k m d \alpha$ をハッシュ関数などで生成し、付加情報 $a j f \alpha$ として転送部16 $\alpha$ に出力する。

なお、付加情報としては、ユーザの秘密鍵で復号化できる暗号化鍵を特定するための、ID、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報であってもよい。

転送部16 $\alpha$ は、入力情報 $M \alpha$ の暗号化に伴って生成された1または複数の暗号化鍵 $E K 1 \alpha$ ,  $E K 2 \alpha$ , ...,  $E K n \alpha$ 、暗号化データ $M' \alpha$ 、および付加情報 $a j f \alpha$ をネットワーク4 $\alpha$ を介して情報保管装置としてのWWWサーバ3 $\alpha$ に転送する。

なお、共通鍵の登録時には転送処理を行わない。

デジタル署名確認部17 $\alpha$ は、WWWサーバ3 $\alpha$ に保管されている特定グループに属する公開鍵のメンバーリスト $G L \alpha$ をネットワーク4 $\alpha$ を介して受けて、チームマスターのデジタル署名を確認し、確認が肯定的である場合、新規にグループに加入するユーザの公開鍵を追加するときは、そ

の公開鍵  $PK$  を記憶部  $13\alpha$  から公開鍵管理部  $18\alpha$  に出力させ、脱会するメンバーがあるときには受け取ったメンバーリストに記載されているメンバーから該当メンバーを削除させ、また、共有鍵を登録するときには、公開鍵  $ID$  リストに応じた公開鍵  $PK\alpha$  を記憶部  $13\alpha$  から暗号化鍵生成部  $14\alpha$  に出力させる。

公開鍵管理部  $18\alpha$  は、新規にグループに加入するユーザの公開鍵を追加するときに、記憶部  $13\alpha$  から出力された指定公開鍵  $PK\alpha$  を受けて、新しいメンバーリストを作成し、公開鍵番号 ( $No$ )、メンバーの公開鍵をリストに設定し、さらに新規のメンバーリストに対してグループ  $ID$  を付加してデジタル署名付加部  $19\alpha$  に出力する。また、たとえば特定グループのメンバーリスト要求等が発生した場合、この要求を  $WWW$  サーバ  $3\alpha$  に対して行う。

デジタル署名付加部  $19\alpha$  は、公開鍵管理部  $18\alpha$  による新規のメンバーリストに対してチームマスターのデジタル署名を付加し、ネットワーク  $4\alpha$  を介して情報保管装置としての  $WWW$  サーバ  $3\alpha$  に転送し、登録させる。

復号化部  $20\alpha$  は、特定グループで共通鍵を共有している場合には、 $WWW$  サーバ  $3\alpha$  に登録されている共通鍵リスト  $CKL\alpha$  の中から所望の共通鍵番号 ( $No$ )、暗号化鍵を取得し、公開鍵暗号方式 (たとえば、 $RSA$ ) を用いてユーザの秘密鍵  $pvk\alpha$  で暗号化鍵を復号して共通鍵を取得し、暗号化部  $11\alpha$  に出力する。

また、 $WWW$  サーバ  $3\alpha$  に登録されているデータを復号する場合には、データ  $ID$ 、公開鍵番号 ( $No$ ) を  $WWW$  サーバ  $3\alpha$  に転送して、暗号化

鍵およびデータを取得し、公開鍵暗号方式を用いて、共通鍵を復号し、共通鍵暗号方式を用いてデータを復号する。

この復号部 20  $\alpha$  は、図 3 に示すように、暗号化鍵復号化部 21  $\alpha$ 、情報復号化部 22  $\alpha$  により構成される。

なお、復号化部 20  $\alpha$  は、たとえば WWW サーバ 3  $\alpha$  に複数の暗号化鍵、付加情報、および暗号化データに加えて保管されている共有鍵暗号方式、公開鍵暗号方式のアルゴリズムを識別するためアルゴリズム識別情報 *desrsa*（たとえば、DES と RSA で暗号化した、など）や、暗号化アルゴリズムの実行に必要な上記以外の情報 *info*（たとえば、DES に利用した初期化乱数など）も、取得する。

そして、たとえば、アルゴリズム識別情報 *desrsa*、情報 *info* に基づいて、復号化に利用できるように、アルゴリズムを初期化する処理等も行う。

WWW サーバ 3  $\alpha$  は、図 4 に示すように、データベースマネジメントシステム (DBMS) 31  $\alpha$  および権限確認機能を有する権限確認部 32  $\alpha$  を有しており、メンバーリスト *GL*  $\alpha$ 、共通鍵リスト *CKL*  $\alpha$ 、グループの共通鍵リスト *GCKL*  $\alpha$ 、暗号化データリスト *EDL*  $\alpha$ 、およびデータ共通鍵リスト *DCKL*  $\alpha$  を所定の記憶部に記録し、保管する。

DBMS 31  $\alpha$  は、図 5 に示すように、メンバーリスト管理部 311  $\alpha$ 、共通鍵管理部 312  $\alpha$ 、および暗号化データ管理部 313  $\alpha$  の 3 つの情報管理保管機能を有している。これらの機能は、権限確認機能を利用して、各変更や登録、データ保管要求が権限を満たしているか否かを確認する。

メンバーリスト管理部 3 1 1  $\alpha$  は、クライアント側からのメンバーリスト変更要求時に、メンバーリスト G L  $\alpha$  にアクセスして、メンバー変更要求に対して応答し、返信されてきたチームマスターの要求に従ってメンバーリスト G L  $\alpha$  を変更する。また、メンバーリスト管理部 3 1 1  $\alpha$  は、グループ全体を追加・削除する機能を有している。

共通鍵管理部 3 1 2  $\alpha$  は、共通鍵登録時に、共通鍵リスト C K L  $\alpha$  とグループの共通鍵リスト G C K L  $\alpha$  にアクセスし、共通鍵の登録を行う。

共通鍵管理部 3 1 2  $\alpha$  は、クライアントからの共通鍵要求に対して、その時点・特定グループでの情報共有に最適な共通鍵（特定グループで複数の共通鍵（随時更新されていく）を有している場合には、最新の共通鍵）を選択して、クライアントに転送する。また、たとえば登録対象の共通鍵に関する暗号化鍵、グループ I D 情報を受信したならば、各リストに振り分けて保管する。そのとき、共通鍵 I D を生成する。

また、特定グループへのメンバーの新規登録時に、新規メンバーが、登録時点よりも前にグループで共有されていた情報を読めるように各リストを変更する場合には、メンバーリスト管理部 3 1 1  $\alpha$  および共通鍵管理部 3 1 2  $\alpha$  は協働して以下に示すような処理を行う。

この場合、メンバーリスト管理部 3 1 1  $\alpha$  は、権限を確認するとともに、グループ I D を参照して特定グループに属するメンバーの公開鍵番号（N o）、公開鍵をメンバーリスト G L  $\alpha$  より取得する。

共通鍵管理部 3 1 2  $\alpha$  は、グループの共通鍵リスト G C K L  $\alpha$  よりグループ I D を参照して、特定グループで利用されている共通鍵番号（N o）を全て検索する。そして、共通鍵リスト C K L  $\alpha$  より、各共通鍵番号（N

o) とチームマスターの公開鍵番号 (No) が一致する全ての暗号化鍵を取得し、クライアントに転送する。

そして、メンバーリスト管理部 3 1 1 α および共通鍵管理部 3 1 2 α は、クライアント側で変更、暗号化等の処理の結果、返信されてきた暗号化鍵とメンバーリスト、公開鍵番号 (No) と共通鍵 ID を受けて、メンバーリスト GL α、共通鍵リスト CKL α、グループの共通鍵リスト GCKL α を変更する。

これにより、新規追加されたメンバーは、共通鍵リストに自分の公開鍵が含まれているので、過去の共有情報を、取得することができる。

また、特定グループからのメンバーの削除時に、削除されたメンバーが、削除以後、グループで共有されていた情報を読めないようにするために各リストを変更する場合、メンバーリスト管理部 3 1 1 α および共通鍵管理部 3 1 2 α は、協働して以下に示すような処理を行う。

この場合、メンバーリスト管理部 3 1 1 α は、メンバーリストの更新を行う。最後の返信部分では、新しいメンバーリストと更新前のメンバーリストとを比較し、削除したメンバーの公開鍵番号 (No) を割り出し、グループ ID と削除したメンバーの公開鍵番号 (No) を共通鍵管理部 3 1 2 α にわたす。

共通鍵管理部 3 1 2 α は、グループの共通鍵リスト GCKL α より、グループ ID を参照して、特定グループで利用されていた共通鍵番号 (No) を全て検索し、共通鍵リスト CKL α より、各共通鍵番号 (No) と削除したメンバーの公開鍵番号 (No) が一致する全ての暗号化鍵を削除する。

なお、DBMS 3 1 α では、メンバーの追加と削除が同時に行われた場

合には、上述した手法が組み合わされて実行される。

暗号化データ保管部 3 1 3  $\alpha$  は、共通鍵管理部 3 1 2  $\alpha$  と協働して、グループの共通鍵リスト G C K L  $\alpha$ 、共通鍵リスト C K L  $\alpha$ 、データ共通鍵リスト D C K L  $\alpha$ 、暗号化データリスト E D L  $\alpha$  をアクセスし、クライアントの要求に従ってメンバーリストの送信と暗号化データの受付を行い、データ I D を生成する。また、復号化要求を受け取った場合には、データ I D と公開鍵番号 (N o) を参照し、3 つのリストを参照して暗号化データと暗号化鍵を返信する。

次に、上記構成による動作を説明する。

なお、ここでは、グループで共通鍵を共有する場合であって、グループへの公開鍵 I D の登録例、共通鍵の登録例、データの暗号化および登録例、共通したいユーザを別途指定する場合の暗号化例、並びにデータの復号化例について、図 6 ～図 1 0 に関連付けて順を追って説明する。

まず、グループで共通鍵を共有する場合であって、グループへの公開鍵 I D の登録例について図 6 に関連付けて説明する。

特定グループに属するメンバーだけで情報を共有したい場合に、まず、グループに属するメンバーの公開鍵 I D の登録が行われる。

この場合、アクセス等の権限の確認が行われ、クライアント側（端末側）から特定グループのメンバーリスト要求が WWW サーバ 3  $\alpha$  に対して、たとえば公開鍵管理部 1 8  $\alpha$  から行われる (S 6 1  $\alpha$ )。

メンバーリスト要求に対して、WWW サーバ 3  $\alpha$  から特定グループに属する公開鍵 I D リストがネットワーク 4  $\alpha$  を介してクライアント側暗号化



復号化装置 10 $\alpha$ に転送される (S 6 2 $\alpha$ )。

暗号化復号化装置 10 $\alpha$ では、デジタル署名確認部 17 $\alpha$ にこの公開鍵リストであるメンバーリストが入力され、ここでチームマスターのデジタル署名の確認が行われる (S 6 3 $\alpha$ )。

確認が肯定的である場合、新規にグループに加入するユーザの公開鍵を追加するときは、その公開鍵 P Kが記憶部 13 $\alpha$ から公開鍵管理部 18 $\alpha$ に出力され、脱会するメンバーがあるときには受け取ったメンバーリストに記載されているメンバーから該当メンバーの公開鍵が削除される (S 6 4 $\alpha$ )。

公開鍵管理部 18 $\alpha$ では、記憶部 13 $\alpha$ から出力された指定公開鍵 P Kを受けて、新しいメンバーリストが作成され (S 6 5 $\alpha$ )、公開鍵番号 (N o)、メンバーの公開鍵、およびグループ I Dがリストに設定されて、デジタル署名付加部 19 $\alpha$ に出力される。

デジタル署名付加部 19 $\alpha$ において、公開鍵管理部 18 $\alpha$ による新規のメンバーリストに対してチームマスターのデジタル署名が付加される (S 6 6 $\alpha$ )。

そして、たとえばデジタル署名付加部 19 $\alpha$ からメンバーリスト更新要求がWWWサーバ 3 $\alpha$ に対して行われ、WWWサーバ 3 $\alpha$ においてメンバーリスト管理部 311 $\alpha$ によりメンバーリスト G L $\alpha$ の更新が行われる (S 6 7 $\alpha$ )。

なお、ステップ S 6 3 $\alpha$ において、デジタル署名確認が否定的である場合には、当該チームマスターはメンバーリスト等の更新、削除等を行う権限のないものとして、ステップ S 6 4 $\alpha$ 以降の処理は行われない。

次に、グループで共通鍵を共有する場合であって、共通鍵の登録例について図 7 に関連付けて説明する。

特定グループに属するメンバーだけで情報を共有したい場合に、そのメンバーで利用する共通鍵の登録が行われる。

この場合、アクセス等の権限の確認が行われ、クライアント側（端末側）から特定グループのメンバーリスト要求が WWW サーバ 3  $\alpha$  に対して、たとえば暗号化鍵生成部 1 4  $\alpha$  から行われる（S 7 1  $\alpha$ ）。

メンバーリスト要求に対して、WWW サーバ 3  $\alpha$  から特定グループに属する公開鍵 ID リストがネットワーク 4  $\alpha$  を介してクライアント側暗号化復号化装置 1 0  $\alpha$  に転送される（S 7 2  $\alpha$ ）。

暗号化復号化装置 1 0  $\alpha$  では、デジタル署名確認部 1 7  $\alpha$  にこの公開鍵リストであるメンバーリストが入力され、ここでチームマスターのデジタル署名の確認が行われる（S 7 3  $\alpha$ ）。

確認が肯定的である場合、公開鍵 ID リストに応じた公開鍵 PK が記憶部 1 3  $\alpha$  から暗号化鍵生成部 1 4  $\alpha$  に出力される。

暗号化鍵生成部 1 4  $\alpha$  では、共通鍵生成部 1 2  $\alpha$  で生成された共通鍵 S k e y 1  $\alpha$  が、与えられた公開鍵を用いてたとえば公開鍵暗号方式に基づいて暗号化され、図 7 に示すように、公開鍵番号、メンバー公開鍵を含む共通鍵リスト用データを付加して 1 または複数の暗号化鍵 E K  $\alpha$  が生成され、転送部 1 6  $\alpha$  に出力される（S 7 4  $\alpha$ ）。

そして、転送部 1 6  $\alpha$  により公開鍵番号、メンバー公開鍵を含む共通鍵リスト用データが付加された暗号化鍵を含む共通鍵リストデータがネットワーク 4  $\alpha$  を介して WWW サーバ 3  $\alpha$  に転送され、共通鍵管理部 3 1 2  $\alpha$

により図 7 に示すように所定の場所に保管される (S 7 5 α)。

なお、転送場 1 6 α から転送される情報には、付加情報生成部 1 5 α で生成された付加情報が含まれる場合もある。

なお、ステップ S 7 3 α において、デジタル署名確認が否定的である場合には、当該チームマスターは共通鍵の登録を行う権限のないものとして、ステップ S 7 4 α 以降の処理は行われぬ。

次に、グループで共通鍵を共有する場合であって、データを暗号化する場合について図 8 に関連付けて説明する。

この場合、アクセス等の権限の確認が行われ、クライアント側 (端末側) から特定グループのメンバーリスト要求、具体的にはグループ ID、ユーザ公開鍵 ID (たとえば番号「IC:FF」) の要求が WWW サーバ 3 α に対して、たとえば暗号化部 1 1 α から行われる (S 8 1 α)。

メンバーリスト要求に対して、WWW サーバ 3 α から特定グループに属する共通鍵 (たとえば「122」)、暗号化鍵 (「zxcv」) がネットワーク 4 α を介してクライアント側暗号化復号化装置 1 0 α に転送される (S 8 2 α)。

暗号化復号化装置 1 0 α では、復号化部 2 0 α において、共通鍵番号 (122)、暗号化鍵 (zxcv) が取得され、公開鍵暗号方式を用いてユーザの秘密鍵 p v k α で暗号化鍵が復号されて共通鍵 S k e y 2 α が取得され、暗号化部 1 1 α に出力される (S 8 3 α, S 8 4 α)。

暗号化部 1 1 α では、入力情報 M α (「こんにちは」) が入力され、この

入力情報 $M_{\alpha}$ が共有鍵暗号方式（たとえば、DES）に基づいて共通鍵 $S_{key\ 2\ \alpha}$ を用いて暗号化され、共通鍵番号（122）が付加された暗号化データ $M'_{\alpha}$ （たとえば「jjjjjjjjjjj」）が生成されて転送部16 $\alpha$ に出力される（S85 $\alpha$ ）。

そして、転送部16 $\alpha$ により共通鍵番号（122）が付加された暗号化データ $M'_{\alpha}$ （たとえば「jjjjjjjjjjj」）がネットワーク4 $\alpha$ を介してWWWサーバ3 $\alpha$ に転送され、暗号化データ管理部313 $\alpha$ により図8に示すように所定の場所に保管される（S86 $\alpha$ ）。

次に、共有したいユーザを別途指定する場合であって、データを暗号化する場合について図9に関連付けて説明する。

この場合、入力情報 $M_{\alpha}$ （「こんにちは」）が暗号化装置10 $\alpha$ の暗号化部11 $\alpha$ に入力される。このとき、共通鍵生成部12 $\alpha$ で、共通鍵 $S_{key\ 1\ \alpha}$ が生成され（S91 $\alpha$ ）、この共通鍵 $S_{key\ 1\ \alpha}$ が暗号化部12 $\alpha$ および暗号化鍵生成部14 $\alpha$ に供給される（S92 $\alpha$ ，S93 $\alpha$ ）。

暗号化部11 $\alpha$ では、入力情報 $M_{\alpha}$ が共有鍵暗号方式DESに基づいて共通鍵 $S_{key\ 1\ \alpha}$ を用いて暗号化され、共通鍵番号（たとえば「124」）が付加された暗号化データ $M'_{\alpha}$ （たとえば「jjjjjjjjjjj」）が生成されて転送部16 $\alpha$ に出力される。

また、暗号化鍵生成部14 $\alpha$ によって、ユーザA、B、Cの公開鍵暗号方式（たとえば、RSA）に基づいた公開鍵 $PK_{\alpha}$ が記憶部13 $\alpha$ から読み出される。

暗号化鍵生成部14 $\alpha$ において、これらそれぞれの公開鍵を利用して、公開鍵暗号方式に基づいて共通鍵 $S_{key\ 1\ \alpha}$ が暗号化され、たとえば暗

号化鍵 (o l k j, O i w i, X k n m) が得られ、公開鍵番号 (「1 1 : A A」、「1 C : F F」、「E 5 : 4 B」) を含むデータが転送部 1 6 α に出力される (S 9 4 α)。

そして、転送部 1 6 α により共通鍵番号 (たとえば「1 2 4」) が付加された暗号化データ M' α (たとえば「jjjjjjjjjjjjj」)、並びに暗号化鍵 (o l k j, O i w i, X k n m)、公開鍵番号 (「1 1 : A A」、「1 C : F F」、「E 5 : 4 B」) を含むデータがネットワーク 4 α を介して WWW サーバ 3 α に転送され、図 9 に示すように所定の場所に保管される (S 9 5 α)。

次に、WWW サーバ 3 α に保管されているデータを取得する場合を、図 1 0 に関連付けて説明する。

この場合、たとえば復号化部 2 0 α からデータ I D (たとえば「4 4 4 4」)、公開鍵 I D が、WWW サーバ 3 α に対して送信される (S 1 0 1 α)。

WWW サーバ 3 α では、受けたデータ I D およびこれに基づく共通鍵番号 (たとえば「1 2 2」) により、暗号化データ (たとえば「jjjjjjjjjjjjj」) およびこれに対応した暗号化鍵 (z x c v) が暗号化データ管理部 3 1 3 α により所定の保管場所から読み出され、ネットワーク 4 α を介してクライアント側へ転送される (S 1 0 2 α)。

復号化部 2 0 α では、公開鍵暗号方式を用いて、公開鍵 I D に対応した秘密鍵を用いて共通鍵が S k e y 2 α として復号される (S 1 0 3 α)。

そして、この共通鍵 S k e y 2 α を用いて、共通鍵暗号方式に基づきデータが「こんにちは」として復号される (S 1 0 4 α)。

次に、特定グループへのメンバーの新規登録時に、新規メンバーが、登録時点よりも前にグループで共有されていた情報を読めるように各リスト

を変更する場合、および特定グループからのメンバーの削除時に、削除されたメンバーが、削除以後、グループで共有されていた情報を読めないようにするために各リストを変更する場合のWWWサーバ3αにおける動作を説明する。

まず、特定グループへのメンバーの新規登録時に、新規メンバーが、登録時点よりも前にグループで共有されていた情報を読めるように各リストを変更する場合について説明する。

この場合、WWWサーバ3αにおいては、メンバーリスト管理部311αにより、権限が確認されるとともに、グループIDを参照して特定グループ（たとえば、Bチーム）に属するメンバーの公開鍵番号（No）、公開鍵がメンバーリストGLαから取得される。

そして、共通鍵管理部312αで、グループの共通鍵リストGCKLαよりグループIDが参照され、特定グループ（たとえば、Bチーム）で利用されている共通鍵番号（たとえば、52、111、123）が全て検索される。

さらに、共通鍵管理部312αにおいて、共通鍵リストCKLαより、各共通鍵番号（たとえば、52、111、123）とチームマスターの公開鍵番号（たとえば、11:AA）が一致する全ての暗号化鍵（たとえば、qwer、peha、gobp）が取得され、チームマスターのクライアントに転送される。

チームマスターの暗号化復号化装置10αでは、メンバーリストと全ての暗号化鍵を復号化した共通鍵（たとえば、Skey100α、Skey105α、Skey80α）が得られる。図6を参照して説明したように、メンバーリストの変更が行れた後、それらの共通鍵が、新規登録されたメ

ンバーの公開鍵を利用して暗号化される（たとえば、xhen、mxco、henc）。

そして、これらの暗号化鍵とメンバーリスト、公開鍵番号（たとえば、L2 : CA）と共通鍵ID（たとえば、52、111、123）がWWWサーバ3αに送信される。

メンバーリスト管理部311αおよび共通鍵管理部312αでは、クライアント側で変更、暗号化等の処理の結果、返信されてきた暗号化鍵とメンバーリスト、公開鍵番号（No）と共通鍵IDを受けて、メンバーリストGLα、共通鍵リストCKLα、グループの共通鍵リストGCKLαが変更される。

これにより、新規追加されたメンバーは、共通鍵リストに自分の公開鍵が含まれているので、過去の共有情報を取得することができるようになる。

次に、特定グループからのメンバーの削除時に、削除されたメンバーが、削除以後、グループで共有されていた情報を読めないようにするために各リストを変更する場合について説明する。

この場合、WWWサーバ3αのメンバーリスト管理部311αでは、メンバーリストの更新が行われる。このとき、最後の返信部分では、新しいメンバーリストと更新前のメンバーリストとが比較され、削除したメンバーの公開鍵番号（No）が割り出される。そして、グループIDと削除したメンバーの公開鍵番号（No）が共通鍵管理部312αにわたされる。

共通鍵管理部312αでは、グループの共通鍵リストGCKLαより、グループIDを参照して、特定グループ（たとえば、Bチーム）で利用されていた共通鍵番号（たとえば、38、444、133）が全て検索される。

次いで、共通鍵管理部 3 1 2  $\alpha$  では、共通鍵リスト C K L  $\alpha$  より、各共通鍵番号（たとえば、3 8、4 4 4、1 3 3）と削除したメンバーの公開鍵番号（たとえば、L L : B B）が一致する全ての暗号化鍵が削除される。

なお、WWWサーバ 3  $\alpha$ 、具体的には、DBMS 3 1  $\alpha$  では、メンバーの追加と削除が同時に行われた場合には、上述した手法が組み合わされて実行される。

以上説明したように、本実施形態によれば、少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されるWWWサーバ 3  $\alpha$  と、情報を見てもよい少なくとも一のメンバーの公開鍵を記憶する記憶部 1 3  $\alpha$  と、情報を暗号化するための共通鍵を用いて上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する暗号化部 1 1  $\alpha$  と、暗号化に用いた共通鍵を、記憶部に記憶され指定された公開鍵で暗号化し、暗号化鍵を生成する暗号化鍵生成部 1 4  $\alpha$  と、複数の暗号化鍵および暗号化データをWWWサーバ 3  $\alpha$  に転送し保管させる転送部 1 6  $\alpha$  と、WWWサーバ 3  $\alpha$  からメンバーリストを取得して、当該メンバーリストのチームマスターのデジタル署名が指定されたデジタル署名と一致するか否かを判断し、一致する場合にのみメンバーの公開鍵の追加または脱会するメンバーの公開鍵の削除を上記記憶部に対して行い、追加登録または削除の場合、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含む新メンバーリストを作成して上記情報保管装置に転送し保管させるリスト管理部 1 7  $\alpha$ 、1 8  $\alpha$ 、1 9  $\alpha$  と、WWWサーバ 3  $\alpha$  から所望の暗号化鍵情報および暗号化データを取得して、この暗号化鍵情報から共通鍵を復号し、復号した共通



鍵で取得した暗号化データを復号する復号化部 20 $\alpha$ とを有する暗号化復号化装置 10 $\alpha$ とをインターネット 4 $\alpha$ で接続したので、グループで共有鍵を共有することができ、暗号化データを保管するデータベースや、サーバ、ファイルシステムの管理者に情報の内容を見られてしまう可能性もない。

したがって、権限のない、サーバ等の情報保管装置の管理者の覗き見、改竄を防ぐことができる。

また、本実施形態では、情報保管装置としてのWWWサーバ 3 $\alpha$ に、クライアント側からのメンバーリスト変更要求時に、メンバーリスト G L $\alpha$ にアクセスして、メンバー変更要求に対して応答し、返信されてきたチームマスターの要求に従ってメンバーリスト G L $\alpha$ を変更可能なメンバーリスト管理部 311 $\alpha$ と、クライアントからの共通鍵要求に対して、その時点・特定グループでの情報共有に最適な共通鍵を選択して、クライアントに転送する共通鍵管理部 312 $\alpha$ と、グループの共通鍵リスト G C K L $\alpha$ 、共通鍵リスト C K L $\alpha$ 、データ共通鍵リスト D C K L $\alpha$ 、暗号化データリスト E D L $\alpha$ をアクセスし、クライアントの要求に従ってメンバーリストの送信と暗号化データの受付を行い、データ I Dを生成し、復号化要求を受け取った場合には、データ I Dと公開鍵番号 (N o)を参照し、3つのリストを参照して暗号化データと暗号化鍵を返信する暗号化データ保管部 313 $\alpha$ とを設けたので、暗号化データを保管するデータベースや、サーバ、ファイルシステム等の情報保管装置を利用して共有されるユーザのデータが覗き見されたり、改竄されるおそれもなく、データの管理を確実に行うことができる。

なお、暗号化複合化装置 10 $\alpha$ におけるメンバーリストの作成、登録、

削除、共通鍵の作成、登録、登録された共通鍵を用いたデータの暗号化、サーバ 3  $\alpha$  に登録されたデータの復号処理工程を実行するためのプログラム、あるいはサーバ 3 におけるリストの変更、登録、保管等のプログラムは、第 1 および第 2 の端末装置（コンピュータ）1  $\alpha$ 、2  $\alpha$  で読み出し可能な記録媒体、たとえば暗号化装置 10  $\alpha$  やサーバ等に設けられたフロッピーディスク、ハードディスク、光ディスク、半導体記憶装置等に記録され、端末装置で読み出されて実行される。

また、他の例としては、たとえばインターネットの専用線や電話回線等の通信線路のように、通信プログラムに伝送する際にこの通信プログラムを一定時間保持するデータ伝送路等を挙げることができる。

また、本実施形態の情報保管装置および暗号化複合化装置 10  $\alpha$  に、送信側から受信側へ情報またはデータが送信された場合、前記送信側から情報またはデータの送信が行われたことを受信側に対し通知する送信通知と、受信側が確実に前記情報を受信したことを送信側に対し通知する受信通知とを行う送受信通知部（図示せず）をさらに備える構成としてもよい。

この構成とすることで、受信者は送受信通知部を利用して受信時（改竄確認および復号後）に、送信者または情報が中継された情報通信装置または情報保管装置に対して、確かに受信した旨を確認するための受信通知を送信することができる。なお、これらの通知に含まれる情報として、送信者から転送された情報の内容（もしくは、その一部）、概要、発信者を特定する情報、受信者を特定する情報、情報取得・保管場所（たとえば URL アドレス、ディレクトリ等）、情報取得日時などがある。

具体的には、情報保管装置では、図 5 の暗号化データ管理部（313  $\alpha$ ）

に、送受信通知部の機能をもたせる。また、暗号化複合化装置では、暗号化に利用したもしくは、復号時に取得できた上述の通知に含まれる情報を利用して送信通知または受信通知を作成し、通信する。通信手段としては、端末に接続されたメールプロトコルや、ブラウザなどが備えるHTTPプロトコルなどの外部の通信機能を代用して利用することができる。

上記構成とするのは、機密性の高い情報（たとえば、契約書等）を通信する場合に、通信の安全性を高めるために、確実に通信を行われたことを送受信者が確認することが望ましいからである。送信者は、送受信通知部を利用して送信時（暗号化時）に、受信者または情報が中継された情報中継装置または情報保管装置に対して、確かに送信した旨を周知するための送信通知を送信することができる。たとえば、HTTP通信で情報の転送を行う場合には、SMTPなど別のプロトコルを利用した通知を転送することによって、通信の存在を送受信両者で確認することにより、より安全性を高めることができる。

以上説明したように、第1の実施形態の発明によれば、グループで共有鍵を共有することができ、暗号化データを保管するデータベースや、サーバ、ファイルシステムの管理者に情報の内容を見られてしまう可能性もない。

#### [第2の実施形態]

第2の実施形態の発明は、例えば、ネットワーク伝送における情報改竄の検知に用いられる情報改竄検知装置および改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

第2の実施形態の発明に関し、従来以下説明する技術が知られている。

従来、情報の改竄を検知する技術（以下、情報改竄検知技術と称する）としては、デジタル署名技術が情報改竄検知装置により実用化されている。一般的なデジタル署名技術の例としては、**Digital Signature Algorithm** や公開鍵暗号方式（例えば RSA方式）とハッシュ関数（例えば、MD 2）と組み合わせるものがある。

図17は、上述した従来の情報改竄検知装置の動作原理を説明する図である。図17に示す情報改竄検知装置は、送信者側に設置された送信端末1βと、該送信端末1βと図示しないネットワーク（インターネット等）を介して接続され、受信者側に設置された受信端末6βとから概略構成されている。この情報改竄検知装置において、暗号化、復号化には、公開鍵および秘密鍵が用いられる。この公開鍵と秘密鍵とは、秘密鍵から公開鍵が計算により求めることができる一方、逆に公開鍵から秘密鍵が計算により求めることができないという関係とされている。

上記構成において、ステップSA1βでは、送信端末1βは、受信端末6βへ送信すべき平文2βを暗号化する。具体的には、送信端末1βは、受信者（受信端末6β）の公開鍵を利用して平文2βから暗号文3βを作成する。次いで、ステップSA2βでは、送信端末1βは、ハッシュ関数を用いて平文2βを圧縮して、MDβ（メッセージダイジェスト）4aβを作成する。

ここで、ハッシュ関数とは、同じ出力値になる任意の2つの異なる入力を発見することが計算量的に実行不可能な関数をいい、デジタル署名等のメカニズムの一部として利用する目的で、長いメッセージから比較的短い

一定値長の圧縮データをハッシュ符号として作成するための一方向関数を用いる。

次に、ステップS A 3  $\beta$  では、送信端末 1  $\beta$  は、送信者（送信端末 1  $\beta$ ）の秘密鍵を利用してM D  $\beta$  4 a  $\beta$  から認証子 5  $\beta$  を作成する。この認証子 5  $\beta$  は、暗号文 3  $\beta$  のもとになる平文 2  $\beta$  に対してされたデジタル署名である。

ここでは、デジタル署名は、メッセージダイジェストの作成という第 1 プロセス、該メッセージダイジェストに対する秘密鍵による暗号化という第 2 プロセスを経てなされるものである。

また、デジタル署名は、上記プロセスの他にメッセージダイジェスト化されていない情報、またはメッセージダイジェストと該情報とを組み合わせたものに対する秘密鍵による暗号化というプロセスを経てなされる場合も含む。

そして、送信端末 1  $\beta$  は、上記暗号文 3  $\beta$  および認証子 5  $\beta$  をネットワークを介して、受信端末 6  $\beta$  へ送信する。これにより、受信端末 6  $\beta$  は、暗号文 3  $\beta$  および認証子 5  $\beta$  を受信した後、まず、ステップS A 4  $\beta$  で受信者（受信端末 6  $\beta$ ）の秘密鍵を利用して暗号文 3  $\beta$  を復号化して、平文 2  $\beta$  を作成する。次いで、ステップS A 5  $\beta$  では、受信端末 6  $\beta$  は、ハッシュ関数を用いて復号化された平文 2  $\beta$  を圧縮することにより、M D  $\beta$  4 b  $\beta$  を作成する。

また、ステップS A 6  $\beta$  では、受信端末 6  $\beta$  は、受信された認証子 5  $\beta$  を送信者（送信端末 1  $\beta$ ）の公開鍵を利用することにより復号化して、M D  $\beta$  4 c  $\beta$  を作成する。

そして、ステップS A 7  $\beta$  では、受信端末 6  $\beta$  は、M D  $\beta$  4 b  $\beta$  とM D

$\beta 4 c \beta$  とを比較することにより、転送情報（暗号文  $3 \beta$  および認証子  $5 \beta$ ）に改竄が行われたか否かの改竄検証を行う。ここで、 $MD \beta 4 b \beta$  と  $MD \beta 4 c \beta$  とが一致している場合には、転送情報に対して改竄が行われていないことを意味する一方、両者が不一致である場合には、転送情報に対して改竄が行われていることを意味する。

ところで、従来の情報改竄検知装置においては、図 17 に示すように、受信した暗号文  $3 \beta$  を復号化する権利を有する受信端末  $6 \beta$  では、転送（送信）途中で転送情報に対して改竄が行われたか否かを、 $MD \beta 4 b \beta$  と  $MD \beta 4 c \beta$  との比較結果から検知することができる。

しかしながら、従来の情報改竄検知装置においては、図 18 に示すように受信した暗号文  $3 \beta$  を復号化する権利を有しない、言い換えれば、受信者の秘密鍵を有しない受信端末  $6 \beta$  では、平文  $2 \beta$  ひいては  $MD \beta 4 b \beta$  を作成することができないため、転送情報に対する改竄検証を行うことができないという欠点があった。

したがって、従来の情報改竄検知装置においては、図 18 に示す受信端末  $6 \beta$  が更に図示しない別の端末へ転送情報を転送した場合、該端末は、たとえ、暗号文  $3 \beta$  を復号化する権利を有していても、改竄がいつどこで行われたかを検知することができない。さらに、従来の情報改竄検知装置においては、最初に転送情報を転送する送信端末  $1 \beta$  がもとの平文  $2 \beta$  より作成された認証子  $5 \beta$ （デジタル署名）でないデジタル署名を転送した場合であっても、上記端末が改竄を検知することができない。つまり、従来の情報改竄検知装置においては、重要な転送情報に対して改竄が行われた場合、改竄が行われた端末（場所）、時間の特定が重要になるが、これ

らの検知・特定を行うことができないのである。

本発明はこのような背景の下になされたもので、受信した情報を復号化する権利を有しない端末であっても、情報の改竄を検知することができる情報改竄検知装置および改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

以下、図面を参照して第2の実施形態について説明する。図11は本発明の一実施形態（第2の実施形態）による情報改竄検知装置の動作原理を説明する図である。この図に示す情報改竄検知装置は、送信者側に設置された端末100βと、該端末100βにインターネット等のネットワークNβを介して接続された端末200βとから概略構成されている。

上記構成において、ステップSB1βでは、端末100βは、ハッシュ関数を用いて転送情報11βを圧縮して、転送情報MDβ（メッセージダイジェスト）12aβを作成する。この転送情報MDβ12aβは、後述するように送信者の転送内容と受信者の受信内容とが相違していないか否かの検証に用いられる。次いで、端末100βは、上記転送情報11βをネットワークNβを介して端末200βへ送信（転送）する。

これにより、端末200βは、転送情報11βを受信した後、ステップSB2βで、ハッシュ関数を用いて転送情報11βを圧縮して、転送情報MDβ12bβを作成する。ここで、転送情報11βに対する改竄が行われていない場合、上記転送情報MDβ12bβと転送情報MDβ12aβとは、同一である。一方、改竄が行われた場合、転送情報MDβ12bβと転送情報MDβ12aβとは、異なる。

そして、ステップSB3 $\beta$ では、端末200 $\beta$ は、受信者（端末200 $\beta$ ）の秘密鍵を利用して転送情報MD $\beta$ 12b $\beta$ を暗号化して、受信内容確認情報13 $\beta$ を生成する。この受信内容確認情報13 $\beta$ は、転送情報MD $\beta$ 12b $\beta$ に対して受信者（端末200 $\beta$ ）によるデジタル署名が行われたものであり、受信者（端末200 $\beta$ ）が転送内容（転送情報11 $\beta$ ）を受信したことを証明する情報である。

ここでは、デジタル署名は、メッセージダイジェスト化、暗号化という2つのプロセスを経てなされたものである。

また、デジタル署名は、上記プロセスの他にメッセージダイジェスト化されていない情報、またはメッセージダイジェストと該情報とを組み合わせたものに対する秘密鍵による暗号化というプロセスを経てなされる場合も含む。

要はデジタル署名は、圧縮されている、いないに関わらずある情報に対して秘密鍵により暗号化されたものである。

次いで、端末200 $\beta$ は、上記受信内容確認情報13 $\beta$ をネットワークN $\beta$ を介して端末100 $\beta$ へ送信する。

これにより、端末100 $\beta$ は、上記受信内容確認情報13 $\beta$ を受信した後、ステップSB4 $\beta$ で、受信者（端末200 $\beta$ ）の公開鍵により受信内容確認情報13 $\beta$ を復号化して、転送情報MD $\beta$ 12c $\beta$ を作成する。次に、ステップSB5 $\beta$ では、端末100 $\beta$ は、転送情報MD $\beta$ 12c $\beta$ と転送情報MD $\beta$ 12a $\beta$ とを比較することにより、改竄が行われたか否かを検証する。具体的には、端末100 $\beta$ は、転送情報MD $\beta$ 12a $\beta$ と転送情報MD $\beta$ 12c $\beta$ とが同一である場合、検証結果を未改竄とする一方、転送情報MD $\beta$ 12a $\beta$ と転送情報MD $\beta$ 12c $\beta$ とが異なる場合、検証



結果を改竄とする。

次に、ステップSB6 $\beta$ では、端末100 $\beta$ は、送信者（端末100 $\beta$ ）の秘密鍵を利用して受信内容確認情報13 $\beta$ を暗号化して、送信内容確認情報14 $\beta$ を作成する。この送信内容確認情報14 $\beta$ は、受信内容確認情報13 $\beta$ に対して送信者（端末100 $\beta$ ）によるデジタル署名が行われたものであり、送信者（端末100 $\beta$ ）が、受信者（端末200 $\beta$ ）の受信した転送内容（転送情報11 $\beta$ ）を送信したことを証明するための情報である。また、送信内容確認情報14 $\beta$ は、受信者（端末200 $\beta$ ）が転送内容（転送情報11 $\beta$ ）を保有してもよいことを証明するための情報である。

図12は、本発明の一実施形態による情報改竄検知装置の具体的な構成を示すブロック図である。この図において、図11の各部に対応する部分には同一の符号を付ける。図12に示す端末100 $\beta$ において、101 $\beta$ は、転送情報11 $\beta$ をネットワークN $\beta$ を介して端末200 $\beta$ へ送信する情報送信部である。102 $\beta$ は、端末200 $\beta$ から送信される受信内容確認情報13 $\beta$ （図11参照）をネットワークN $\beta$ を介して受信する情報受信部である。

103 $\beta$ は、図11に示すステップSB1 $\beta$ 、SB4 $\beta$ およびSB5 $\beta$ の処理を実行する受信内容確認情報確認部であり、メッセージダイジェスト作成部103a $\beta$ 、送信者・通信・受信者情報取得部103b $\beta$ およびデジタル署名確認部103c $\beta$ とを有している。受信内容確認情報確認部103 $\beta$ において、メッセージダイジェスト作成部103a $\beta$ は、図11に示すステップSB1 $\beta$ の処理を実行するものであり、転送情報11 $\beta$ を

ハッシュ関数で圧縮して転送情報MD  $\beta$  1 2 a  $\beta$ を作成する。送信者・通信・受信者情報取得部 1 0 3 b  $\beta$ は、転送情報 1 1  $\beta$ 、受信内容確認情報 1 3  $\beta$ から各送信者情報、通信情報、受信者情報を取得する。

ここで、送信者情報は、送信者（端末 1 0 0  $\beta$ ）に関する情報であり、「送信者名」、「ID」、「公開鍵 ID」、「メールアドレス」、信頼性が高い第三者機関によって発行された「電子証明書」等の情報である。また、通信情報は、端末 1 0 0  $\beta$ と端末 2 0 0  $\beta$ との間の通信に関する情報であり、「通信時間」、「受信時間」、「通信方式」、「通信 ID」等の情報である。また、受信者情報は、受信者（端末 2 0 0  $\beta$ ）に関する情報であり、「受信者名」、「ID」、「公開鍵 ID」、「メールアドレス」、信頼性が高い第三者機関によって発行された「電子証明書」等の情報である。

図 1 2 に示すデジタル署名確認部 1 0 3 c  $\beta$ は、受信内容確認情報 1 3  $\beta$ （図 1 1 参照）のデジタル署名が受信者（端末 2 0 0  $\beta$ ）によるものであるかを確認する。

1 0 4  $\beta$ は、図 1 1 に示すステップ S B 6  $\beta$ 等の処理を実行する送信内容確認情報作成部であり、メッセージダイジェスト作成部 1 0 4 a  $\beta$ 、送信者・通信・受信者情報取得部 1 0 4 b  $\beta$ およびメッセージダイジェスト作成部 1 0 4 a  $\beta$ とを有している。この送信内容確認情報作成部 1 0 4  $\beta$ は、受信内容確認情報 1 3  $\beta$ に基づいて、送信内容確認情報 1 4  $\beta$ を作成する。

この送信内容確認情報作成部 1 0 4  $\beta$ において、メッセージダイジェスト作成部 1 0 4 a  $\beta$ は、受信内容確認情報 1 3  $\beta$ からメッセージダイジェストを作成する。送信者・通信・受信者情報取得部 1 0 4 b  $\beta$ は、上述し

た送信者・通信・受信者情報取得部 103b $\beta$ と同様にして、受信内容確認情報 13 $\beta$ から送信者情報、通信情報および受信者情報を取得する。デジタル署名付加部 104c $\beta$ は、受信内容確認情報 13 $\beta$ を送信者（端末 100 $\beta$ ）の秘密鍵により暗号化することにより、受信内容確認情報 13 $\beta$ に対してデジタル署名を付加する。

105 $\beta$ は、ネットワーク N $\beta$ を介して送信内容確認情報 14 $\beta$ を端末 200 $\beta$ へ送信する情報送信部である。

一方、端末 200 $\beta$ において、201 $\beta$ は、端末 100 $\beta$ からネットワーク N $\beta$ を介して送信される転送情報 11 $\beta$ を受信する情報受信部である。202 $\beta$ は、図 11 に示すステップ SB2 $\beta$ および SB3 $\beta$ の処理を実行する受信内容確認情報作成部であり、メッセージダイジェスト作成部 202a $\beta$ 、送信者・通信・受信者情報取得部 202b $\beta$ およびデジタル署名付加部 202c $\beta$ とを有している。この受信内容確認情報作成部 202 $\beta$ は、転送情報 11 $\beta$ に基づいて受信内容確認情報 13 $\beta$ を作成する。

この受信内容確認情報作成部 202 $\beta$ において、メッセージダイジェスト作成部 202a $\beta$ は、転送情報 11 $\beta$ をハッシュ関数で圧縮することにより、転送情報 MD $\beta$ 12b $\beta$ （図 11 参照）を作成する。送信者・通信・受信者情報取得部 202b $\beta$ は、上述した送信者・通信・受信者情報取得部 103b $\beta$ と同様にして、転送情報 11 $\beta$ に関する送信者情報、通信情報および受信者情報を取得する。デジタル署名付加部 202c $\beta$ は、転送情報 MD $\beta$ 12b $\beta$ （図 11 参照）を受信者（端末 200 $\beta$ ）の秘密鍵により暗号化することにより、転送情報 MD $\beta$ 12b $\beta$ に対してデジタル署名を付加する。ここで、このデジタル署名が付加された転送情報 MD $\beta$ 12b $\beta$ は、受信内容確認情報 13 $\beta$ である。

また、205βは、端末100βから送信された送信内容確認情報14βの内容を転送情報11βに基づいて確認する送信内容確認情報確認部であり、メッセージダイジェスト作成・取得部205aβと、送信者・通信・受信者情報取得部205bβと、デジタル署名確認部205cβとを有している。この送信内容確認情報確認部205βにおいて、メッセージダイジェスト作成・取得部205aβは、上述したメッセージダイジェストを作成する機能と、受信内容確認情報作成部202βのメッセージダイジェスト作成部202aβによりすでに作成された転送情報MDβ12bβ（図11参照）を取得する機能とを有する。ここで、上記転送情報MDβ12bβを取得した場合には、メッセージダイジェスト作成・取得部205aβは、メッセージダイジェストを作成しない。送信者・通信・受信者情報取得部205bβは、上述した送信者・通信・受信者情報取得部103βと同様にして、送信者情報、通信情報および受信者情報を取得する。デジタル署名確認部205cβは、送信者（端末100β）の公開鍵を用いて、受信内容確認情報13βに対するデジタル署名を確認する。

次に、上述した一実施形態による情報改竄検知装置の動作について図13～図16に示すフローチャートを参照しつつ説明する。図13は、図12に示す受信内容確認情報確認部103βの動作を説明するフローチャートであり、図14は、図12に示す送信内容確認情報作成部104βの動作を説明するフローチャートである。また、図15は、図12に示す受信内容確認情報作成部202βの動作を説明するフローチャートであり、図16は、図12に示す送信内容確認情報確認部205βの動作を説明するフローチャートである。

図 1 2 において、端末 1 0 0  $\beta$  における転送情報 1 1  $\beta$  が情報送信部 1 0 1  $\beta$  によりネットワーク N  $\beta$  を介して端末 2 0 0  $\beta$  へ送信されると、該転送情報 1 1  $\beta$  は、端末 2 0 0  $\beta$  の情報受信部 2 0 1  $\beta$  により受信される。これにより、端末 2 0 0  $\beta$  の受信内容確認情報作成部 2 0 2  $\beta$  は、図 1 5 に示すフローチャートに従って受信内容確認情報 1 3  $\beta$  を生成する。

具体的には、図 1 5 に示すステップ S E 1  $\beta$  では、受信内容確認情報作成部 2 0 2  $\beta$  は、受信内容（転送情報 1 1  $\beta$ ）を入力する。これにより、ステップ S E 2  $\beta$  では、メッセージダイジェスト作成部 2 0 2 a  $\beta$  は、受信内容（転送情報 1 1  $\beta$ ）をハッシュ関数で圧縮してメッセージダイジェスト（図 1 1 : 転送情報 M D  $\beta$  1 2 b  $\beta$ ）を作成する。なお、図 1 5 に示す例では、ステップ S E 2  $\beta$  の処理を実行することなく、ステップ S E 1  $\beta$  からステップ S E 6  $\beta$  へ進んでもよい。

また、ステップ S E 3  $\beta$  ~ S E 5  $\beta$  では、受信内容確認情報作成部 2 0 2  $\beta$  は、送信者情報（送信者名、I D、公開鍵 I D、メールアドレス、電子証明書等）、受信者情報（受信者名、I D、公開鍵 I D、メールアドレス、電子証明書等）、通信情報（送信時間、受信時間、通信方式、通信 I D 等）を転送情報 1 1  $\beta$  から取り込む。

これにより、ステップ S E 6  $\beta$  では、送信者・通信・受信者情報取得部 2 0 2 b  $\beta$  は、ステップ S E 3  $\beta$  ~ S E 5  $\beta$  で入力された送信者情報、受信者情報および通信情報を取得した受信内容確認情報作成部 2 0 2  $\beta$  は、上述した受信内容（転送情報 1 1  $\beta$ ）と、転送情報 M D  $\beta$  1 2 b  $\beta$ 、送信者情報、受信者情報、通信情報等の各情報とを統合する。ここで、情報の統合とは、ハッシュ関数で圧縮された転送情報 M D  $\beta$  1 2 b  $\beta$  の全部

または一部と、送信者情報における送信者名、ID等、受信者情報における受信者名、ID等、通信情報における送信時間、受信時間等のうち1つまたは複数の情報とを組み合わせることをいう。

次に、ステップSE7βでは、メッセージダイジェスト作成部202aβは、ステップSE6βで統合された情報をハッシュ関数で圧縮することにより、メッセージダイジェストを作成する。次いで、ステップSE8βでは、デジタル署名付加部202cβは、ステップSE7βで作成されたメッセージダイジェストを受信者の秘密鍵で暗号化することにより、メッセージダイジェストに対して、デジタル署名を付加する。そして、ステップSE9βでは、受信内容確認情報作成部202βは、各情報を統合化することにより、図11に示す受信内容確認情報13βを作成した後、これを情報送信部203βへ出力する。

また、メッセージダイジェスト作成部202aβは、必要に応じて転送情報MDβ12bβを送信内容確認情報確認部205βのメッセージダイジェスト作成・取得部205aβへ出力する。この場合、メッセージダイジェスト作成・取得部205aβは、メッセージダイジェストの作成を行うことなく、上記転送情報MDβ12bβを取得する。

そして、上記受信内容確認情報13βは、情報送信部203βによりネットワークNβを介して端末100βへ送信された後、端末100βの情報受信部102βにより受信される。これにより、端末100βの受信内容確認情報確認部103βは、図13に示すフローチャートに従って、受信内容確認情報13βの内容を確認することにより、改竄を検知する。

具体的には、図13に示すステップSC1βでは、受信内容確認情報確

認部 1 0 3  $\beta$  は、情報受信部 1 0 2  $\beta$  により受信された受信内容確認情報 1 3  $\beta$  を入力した後、ステップ S C 2  $\beta$  へ進む。ステップ S C 2  $\beta$  では、メッセージダイジェスト作成部 1 0 3 a  $\beta$  は、受信者の公開鍵を用いて受信内容確認情報 1 3  $\beta$  を復号化することにより、メッセージダイジェスト（図 1 1 : 転送情報 M D  $\beta$  1 2 c  $\beta$ ）を作成（取得）する。

そして、ステップ S C 3  $\beta$  では、デジタル署名確認部 1 0 3 c  $\beta$  は、受信者（端末 2 0 0  $\beta$ ）の公開鍵を用いて、受信内容確認情報 1 3  $\beta$  が受信者によりデジタル署名されたものであるか否かを確認する。ここで、受信内容確認情報 1 3  $\beta$  が受信者（端末 2 0 0  $\beta$ ）の公開鍵で復号化できた場合、受信内容確認情報 1 3  $\beta$  は、受信者によりデジタル署名されたものであり、一方、受信内容確認情報 1 3  $\beta$  が受信者の公開鍵で復号化できなかった場合、受信内容確認情報 1 3  $\beta$  は受信者によりデジタル署名されなかったものである。

次に、ステップ S C 4  $\beta$  では、受信内容確認情報確認部 1 0 3  $\beta$  は、ステップ S C 3  $\beta$  の確認結果から、受信内容確認情報 1 3  $\beta$  のデジタル署名が受信者（端末 2 0 0  $\beta$ ）のデジタル署名であるか否かを判断し、同判断結果が「NO」の場合、改竄もしくは通信エラーが発生したものとする。一方、ステップ S C 4  $\beta$  の判断結果が「YES」の場合、受信内容確認情報確認部 1 0 3  $\beta$  は、ステップ S C 5  $\beta$  へ進む。

ステップ S C 5  $\beta$  では、受信内容確認情報 1 3  $\beta$  に含まれている各種情報を分類する。ここで、上記各種情報としては、受信情報内容、前述した送信者情報、受信者情報、通信情報、メッセージダイジェスト（転送情報 M D  $\beta$  1 2 c  $\beta$ ）等がある。

また、受信内容確認情報確認部 1 0 3  $\beta$  は、ステップ S C 6  $\beta$  へ進み、転送情報 1 1  $\beta$ 、送信者が転送した、通信に関する送信者情報、通信情報、受信者情報等を入力する。次に、ステップ S C 7  $\beta$  では、受信内容確認情報確認部 1 0 3  $\beta$  のメッセージダイジェスト作成部 1 0 3 a  $\beta$  は、転送情報 1 1  $\beta$  をハッシュ関数で圧縮して転送情報 M D  $\beta$  1 2 a  $\beta$  (図 1 1 参照) を作成する。

そして、受信内容確認情報確認部 1 0 3  $\beta$  は、ステップ S C 9  $\beta$  ~ S C 1 2  $\beta$  で受信内容と送信内容とを比較することにより、受信内容の検証を情報毎に行う。そして、ステップ S C 1 3  $\beta$  では、受信内容確認情報確認部 1 0 3  $\beta$  は、上記ステップ S C 9  $\beta$  ~ S C 1 2  $\beta$  の検証結果を受けて、受信内容が送信内容と相違ないか否かを判断し、同判断結果が「N O」の場合、改竄もしくは通信エラーが発生しているものとする。一方、受信内容確認情報確認部 1 0 3  $\beta$  は、受信内容が送信内容と相違していない場合、S C 1 3  $\beta$  の判断結果を「Y E S」として、改竄が発生していないものとする。

次いで、送信内容確認情報作成部 1 0 4  $\beta$  は、図 1 4 に示すフローチャートに従って、送信内容確認情報 1 4  $\beta$  (図 1 1 参照) を作成する処理を実行する。すなわち、送信内容確認情報作成部 1 0 4  $\beta$  は、図 1 4 に示すステップ S D 1  $\beta$  で受信内容確認情報 1 3  $\beta$  を入力した後、ステップ S D 2  $\beta$  で受信内容確認情報承認情報を生成する。ここで、受信内容確認情報承認情報とは、受信内容確認情報確認部 1 0 3  $\beta$  が受信内容確認情報 1 3  $\beta$  の内容を承認(確認)した旨を示す情報である。この承認(確認)した旨を示す情報は、承認した時間、端末、承認者(一実施形態では送信者)



に関する情報を元に生成される。

次いで、ステップSD3 $\beta$ では、送信内容確認情報作成部104 $\beta$ は、受信内容確認情報13 $\beta$ と受信内容確認情報承認情報とを統合する。次に、ステップSD4 $\beta$ では、メッセージダイジェスト作成部104a $\beta$ は、ステップSD3 $\beta$ において統合された情報のメッセージダイジェストを取得した後、ステップSD5 $\beta$ へ進む。ステップSD5 $\beta$ では、デジタル署名付加部104c $\beta$ は、送信者（端末100 $\beta$ ）の秘密鍵により暗号化することにより、メッセージダイジェストに対してデジタル署名を行う。

そして、ステップSD6 $\beta$ では、送信内容確認情報作成部104 $\beta$ は、ステップSD3 $\beta$ における各種情報とステップSD5 $\beta$ においてデジタル署名されたメッセージダイジェストとを統合化する。これにより、送信内容確認情報作成部104 $\beta$ においては、送信内容確認情報14 $\beta$ が作成され、該送信内容確認情報14 $\beta$ は、情報送信部105 $\beta$ へ出力される。

そして、上記送信内容確認情報14 $\beta$ は、情報送信部105 $\beta$ により、ネットワークN $\beta$ を介して端末200 $\beta$ へ送信された後、端末200 $\beta$ の情報受信部204 $\beta$ により受信される。

これにより、端末200 $\beta$ の送信内容確認情報確認部205 $\beta$ は、図16に示すフローチャートに従って、送信内容確認情報14 $\beta$ の確認を実行する。

具体的には、図16に示すステップSF1 $\beta$ では、送信内容確認情報確認部205 $\beta$ は、情報受信部204 $\beta$ により受信された送信内容確認情報14 $\beta$ を入力した後、ステップSF2 $\beta$ へ進む。ステップSF2 $\beta$ では、

メッセージダイジェスト作成・取得部 205 a  $\beta$  は、送信者（端末 100  $\beta$ ）の公開鍵を用いて送信内容確認情報 14  $\beta$  を復号化することにより、メッセージダイジェストを作成（取得）する。

そして、ステップ S F 3  $\beta$  では、デジタル署名確認部 205 c  $\beta$  は、送信者（端末 100  $\beta$ ）の公開鍵を用いて、送信内容確認情報 14  $\beta$  が送信者によりデジタル署名されたものであるか否かを確認する。ここで、送信内容確認情報 14  $\beta$  が送信者（端末 100  $\beta$ ）の公開鍵で復号化できた場合、送信内容確認情報 14  $\beta$  は、送信者によりデジタル署名されたものであり、一方、送信内容確認情報 14  $\beta$  が送信者の公開鍵で復号化できなかった場合、送信内容確認情報 14  $\beta$  は送信者によりデジタル署名されなかったものである。

次に、ステップ S F 4  $\beta$  では、送信内容確認情報確認部 205  $\beta$  は、ステップ S F 3  $\beta$  の確認結果から、送信内容確認情報 14  $\beta$  のデジタル署名が送信者（端末 100  $\beta$ ）のデジタル署名であるか否かを判断し、同判断結果が「NO」の場合、改竄もしくは通信エラーが発生したものとする。一方、ステップ S F 4  $\beta$  の判断結果が「YES」の場合、送信内容確認情報確認部 205  $\beta$  は、ステップ S F 5  $\beta$  へ進む。

ステップ S F 5  $\beta$  では、送信内容確認情報 14  $\beta$  に含まれている各種情報を分類する。ここで、上記各種情報としては、受信情報内容、前述した送信者情報、受信者情報、通信情報、メッセージダイジェスト等がある。

また、送信内容確認情報確認部 205  $\beta$  は、ステップ S F 6  $\beta$  へ進み、受信した転送情報 11  $\beta$ 、送信者が転送した、通信に関する送信者情報、

通信情報、受信者情報等を入力する。次に、ステップSF7 $\beta$ では、送信内容確認情報確認部205 $\beta$ のメッセージダイジェスト作成・取得部205a $\beta$ は、転送情報11 $\beta$ をハッシュ関数で圧縮して転送情報MD $\beta$ 12b $\beta$ （メッセージダイジェスト）を作成する。ただし、メッセージダイジェスト作成・取得部205a $\beta$ は、メッセージダイジェスト作成部202a $\beta$ から転送情報MD $\beta$ 12b $\beta$ を取得した場合、上記作成動作を行わない。

そして、送信内容確認情報確認部205 $\beta$ は、ステップSF9 $\beta$ ～SF12 $\beta$ で受信内容と送信内容とを比較することにより、受信内容の検証を情報毎に行う。そして、ステップSF13 $\beta$ では、送信内容確認情報確認部205 $\beta$ は、上記ステップSF9 $\beta$ ～SF12 $\beta$ の検証結果を受けて、受信内容が送信内容と相違ないか否かを判断し、同判断結果が「NO」の場合、改竄もしくは通信エラーが発生しているものとする。一方、送信内容確認情報確認部205 $\beta$ は、受信内容が送信内容と相違していない場合、SF13 $\beta$ の判断結果を「YES」として、改竄が発生していないものとする。

以上説明したように、上述した一実施形態による情報改竄検知装置によれば、受信内容確認情報13 $\beta$ 、送信内容確認情報14 $\beta$ を用いて改竄検知を行うように構成したので、受信した情報を復号化する権利を有しない端末であっても、情報の改竄を検知することができる。

以上第2の実施形態について詳述してきたが、具体的な構成はこの実施形態に限定されるものではない。例えば、上述した一実施形態による情報改竄検知装置においては、上述した機能を実現するための改竄検知プログ

ラムを、コンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録された改竄検知プログラムをコンピュータシステムに読み込ませて実行させることにより、情報の改竄検知をおこなってもよい。

また、上記改竄検知プログラムは、フロッピーディスク、CD-ROM等の可搬媒体や、ハードディスク等の記憶装置等に、その全体あるいは一部が記録され

、あるいは記憶されている。その改竄検知プログラムは、コンピュータにより読みとられて、動作の全部あるいは一部が実行される。

また、ここでいう記録媒体は、光磁気ディスク等のように改竄検知プログラムを静的に記録しているものに限らず、インターネットの専用線、電話回線等の通信回線を通して改竄検知プログラムを送信する場合の通信回線のように、短時間の間、動的に改竄検知プログラムを保持しているもの、その場合のサーバやコンピュータ内部のメモリのように、一定時間改竄検知プログラムを保持しているものも含むものとする。

以上説明したように、第2の実施形態の発明によれば、受信内容確認情報、送信内容確認情報を用いて改竄検知を行うように構成したので、受信した情報を復号化する権利を有しない端末であっても、情報の改竄を検知することができる。

### [第3の実施形態]

第3の実施形態の発明は、情報の暗号化復号化を行なう暗号化装置、復号化装置、方法及びその記録媒体に関する。

第3の実施形態の発明に関し、従来以下説明する技術が知られている。

一般に情報の伝達に際し、この情報に秘匿性が要求される場合がある。そこでさまざまな暗号化方式が考案されている。ここで従来の暗号化・署名方式を用いた暗号化装置の1例の動作フローチャートを図33に示す。この例の方式では、公開鍵暗号方式と共通鍵暗号方式を組み合わせ利用している。

まず、暗号化装置は、送信者による共通鍵の入力か、または暗号化装置側で乱数を発生させ共通鍵を生成し共通鍵を取得する（ステップS151 $\gamma$ ）。

次に、公開鍵暗号方式を利用し受信者の公開鍵を用いて共通鍵を暗号化し暗号化鍵とする（ステップS152 $\gamma$ ）。

次に共通鍵暗号化方式を利用し、平文を共通鍵を用いて暗号化し暗号文を生成する（ステップS153 $\gamma$ ）。

さらにハッシュ関数を用いて平文を圧縮することでメッセージダイジェストであるMD $\gamma$ を作成する（ステップS154 $\gamma$ ）。

そして、このMD $\gamma$ を送信者の秘密鍵で暗号化することでデジタル署名を付加する（ステップS155 $\gamma$ ）。

送信者は、以上で生成した暗号化鍵と暗号文とデジタル署名をネットワーク等を介して受信者に送信する。

図34に、上記暗号化・デジタル署名方式に対応する復号化方式を用いた復号化装置の動作フローチャートを示す。

復号化装置は、暗号化鍵と暗号文とデジタル署名を受信すると、まず受信者の秘密鍵を利用して暗号化鍵を復号化し共通鍵を得る（ステップS161 $\gamma$ ）。

そしてこの共通鍵を用いて暗号文を復号化し平文を得る（ステップS162 $\gamma$ ）。

次に復号化して得た平文をハッシュ関数で圧縮しメッセージダイジェストMD

$\gamma$ を生成する（ステップS163 $\gamma$ ）。

さらに受信したメッセージダイジェストMD $\gamma$ のデジタル署名を送信者の公開鍵で復号化しMD $\gamma$ を得る（ステップS164 $\gamma$ ）。

次に、このMD $\gamma$ と先のMD' $\gamma$ を比較し、元の平文が改竄されていないかの検証を行なっている。この方式の場合、著名検証により平文への著名者を本人確認できる利点がある。

次に、特開平8-156964に開示されている暗号化方式では、平文であるデータパーツが複数からなる情報を上記方式で暗号化している。図35にn個のデータパーツ（平文）からなる情報と、この情報から生成される暗号化情報の構成を示している。この場合の暗号化情報は、各データパーツに対応する暗号化鍵とデータパーツの暗号文とデータパーツのデジタル署名を含んでいる。一例として69バイトのデータパーツに対して付加されるデジタル署名のサイズは、2329バイトである。デジタル署名のサイズには下限がありデータパーツのサイズが小さくてもデジタル署名はあるサイズ以上の大きさをもつ。例えば、69バイトのデータパーツ100個から構成される情報に対し、改竄防止のためにデジタル署名を付加すると、 $2329 \times 100 = 232900$ バイトの情報が付加されることになる。

次に、特開平9-71388に開示されている暗号化方式では、複数のデータパーツからなる情報に対して、各データパーツのメッセージダイジェストをまとめてデジタル署名し暗号化している。図36にn個のデータパーツ（平文）からなる情報と、この情報から生成される暗号化情報の構

成を示している。

複数のデータパーツからなる情報を暗号化する場合、例えば特開平 8-156964 に開示されている方式では、データのオーバーヘッドが大きくなり、暗号化情報の伝送により多くの時間がかかることや、記憶装置等の資源を多く必要とする等の問題がある。また、特開平 9-71388 に開示されている方式では、各データパーツのメッセージダイジェストをまとめてデジタル署名しているので、すべての平文がそろわないとデジタル署名の確認ができず、一部のデータパーツの参照のみ許可されているユーザがいる場合、データパーツの改竄を検証することができない点や、各データパーツを同時に変更できない等の問題がある。

本発明は、上記の点に鑑みてなされたもので、複数のデータパーツ（平文）を含む情報を暗号化した暗号化情報のオーバーヘッドをより少なくでき、また複数のユーザで利用可能であるとともに、各データパーツの改竄検証と同時変更も可能な暗号化装置、復号化装置、方法及びその記録媒体を提供するものである。

以下、第 3 の実施形態を図面を参照して説明する。

図 19 は、本発明の一実施形態である暗号化装置、復号化装置の構成を示すブロック図である。なお、本実施の形態では、暗号化装置と復号化装置とが一体となった暗号化復号化装置として説明する。

本実施形態の暗号化復号化装置 10 γ は、鍵暗号化部 11 γ と、鍵復号化部 12 γ と、暗号化部 13 γ と、復号化部 14 γ とを備える。鍵暗号化部 11 γ は、共通鍵取得部 15 γ と共通鍵暗号化部 16 γ と第 1 共通鍵改

竄検出情報作成部としての共通鍵改竄検出情報作成部 17 γ からなる。鍵復号化部 12 γ は、共通鍵復号化部 18 γ と第 2 共通鍵改竄検出情報作成部としての共通鍵改竄情報作成部 19 γ と第 1 改竄検証部としての改竄検証部 20 γ からなる。暗号化部 13 γ は、データ暗号化部 21 γ と第 1 データ改竄検出情報作成部としてのデータ改竄検出情報作成部 22 γ からなる。復号化部 14 γ は、データ復号化部 23 γ と第 2 データ改竄検出情報作成部としてのデータ改竄検出情報作成部 24 γ と第 2 改竄検証部としての改竄検証部 25 γ からなる。

共通鍵取得部 15 γ は、暗号化に使用する共通鍵を取得または生成する。共通鍵の生成には、一例として乱数生成装置等を利用し生成させる。共通鍵暗号化部 16 γ は、RSA 方式や楕円暗号方式等の公開鍵暗号方式を利用して共通鍵を暗号化する。暗号化に使用する公開鍵は、情報を共有するメンバーの公開鍵を使用する。例えば共有メンバーが 3 人の場合、3 人が所持する公開鍵を用いて共通鍵を暗号化し、3 つの暗号化鍵を作成する。共通鍵改竄検出情報作成部 17 γ は、共通鍵の正当性（1. 改竄されていない、2. 正当なユーザによって作成されている等）を検証するために利用する鍵情報を作成する。一例として、共通鍵を MD5、SHA-1 等のハッシュ関数で圧縮して共通鍵のメッセージダイジェスト MD γ を作成し、この MD γ に共通鍵作成者の秘密鍵を用いてデジタル署名を行なったものを鍵情報として利用できる。デジタル署名の作成・検証には、公開鍵暗号方式の他、DSA 等のデジタル署名方式等を利用してよい。

共通鍵復号化部 18 γ は、共通鍵暗号化部 16 γ により暗号化された暗号化鍵を公開鍵暗号方式を用いて復号化する。復号化に用いる秘密鍵は、復号化を行なうユーザの秘密鍵を用いる。共通鍵改竄検出情報作成部 19



γ は、共通鍵の正当性確認を行なうために利用する共通鍵改竄検出情報を作成する。例えば、共通鍵復号化部 18 γ で復号化された共通鍵をハッシュ関数で圧縮したメッセージダイジェスト MD' γ を作成する。改竄検証部 20 γ は、鍵情報（一例として MD γ）と共通鍵改竄検出情報作成部 19 γ で作成した共通鍵改竄検出情報（一例として MD' γ）を比較検証することにより、共通鍵の正当性を確認する。共通鍵の正当性を確認するにあたり、共通鍵作成者自身の正当性確認も必要となるが、別途定められるものである。

データ暗号化部 21 γ は、データパーツ（平文）を共通鍵暗号方式を利用して暗号化し、暗号文を生成する。暗号化に使用する共通鍵は、初めて暗号化する場合には共通鍵取得部 15 γ で取得または生成された共通鍵を用い、既存の暗号化情報を利用する場合には、共通鍵復号化部 18 γ により復号化された共通鍵を用いる。データ改竄検出情報作成部 22 γ は、データパーツが改竄されていないか検証するための第 1 データ改竄検出情報を作成する。例えば、ハッシュ関数を用いてデータパーツを圧縮したメッセージダイジェストや、データパーツから抽出した部分情報、ID 番号などを第 1 データ改竄検出情報として利用できる。

データ復号化部 23 γ は、共通鍵暗号方式を用いて暗号文を復号化する。復号化に用いる共通鍵は、共通鍵復号化部 18 γ により復号化された共通鍵を用いる。データ改竄検出情報作成部 24 γ は、第 1 データ改竄検出情報に対応しデータパーツが改竄されていないか検証するための第 2 データ改竄検出情報を作成する。例えば、データ復号化部 23 γ で復号化された元のデータパーツをハッシュ関数を用いて圧縮して作成したメッセージダイジェストや、データパーツから抽出した部分情報、ID 番号などを第

2 データ改竄検出情報として利用できる。改竄検証部 25 γ は、第 1 データ改竄検出情報と第 2 データ改竄検出情報を比較検証することにより、復号化した元のデータパーツの正当性を確認する。

なお、共通鍵暗号化部 16 γ とデータ暗号化部 21 γ を、同一の装置で実現してもよい。また、共通鍵復号化部 18 γ とデータ復号化部 23 γ を、同一の装置で実現してもよい。また、共通鍵改竄検出情報作成部 17 γ と 19 γ、または、データ改竄検出情報作成部 22 γ と 24 γ を、同一の装置で実現してもよい。同様に、共通鍵改竄検出情報作成部 17 γ と 19 γ 及びデータ改竄検出情報作成部 22 γ と 24 γ のすべてを、同一の装置で実現してもよい。また、改竄検証部 20 γ と改竄検証部 25 γ を、同一の装置で実現してもよい。また、本実施の形態の暗号化復号化装置を、単一の装置としてではなく、各部が独立した装置として実現し利用してもよい。なお、請求項 51 および請求項 52 に記載の暗号化装置は、鍵暗号化部 11 γ と暗号化部 13 γ とから構成できる。また、請求項 53 に記載の暗号化装置は、鍵暗号化部 11 γ と暗号化部 13 γ と鍵復号化部 12 γ とから構成できる。請求項 54 および請求項 55 に記載の復号化装置は、鍵復号化部 12 γ と復号化部 14 γ とから構成できる。

図 20 に、本実施形態の暗号化復号化装置 10 γ の一利用形態を示す。

本利用形態では、ネットワークに接続可能なサーバや他端末装置等からなる情報保管装置 30 γ と、暗号化復号化装置 10 γ を備える端末装置 31 γ とがネットワークを介して接続されている。情報保管装置 30 γ は、ハードディスク、光磁気ディスク等の不揮発性の記録装置を備え、暗号化情報として、暗号文、データ改竄検出情報、暗号化鍵、鍵情報および関連情報を保存可能とする。また、端末装置 31 γ には、周辺機器として入力

装置、表示装置等（いずれも図示せず）が接続されるものとする。ここで、入力装置とはキーボード、マウス等の入力デバイスのことをいう。表示装置とはCRT（Cathode Ray Tube）や液晶表示装置等のことをいう。なお、暗号化情報をローカルな端末装置31γに保管し、スタンドアローンで利用してもよい。

次に、このように構成された利用形態における本実施形態の暗号化復号化装置10γの動作について説明する。

まず、最初のデータパーツを暗号化する際の暗号化復号化装置10γの動作を図21に示す動作フローチャートを参照して説明する。なお、下記の説明における動作手順は、本実施形態の動作の一例であり、その処理の順序は固定されるものではなく他の順序で実施されてもよい。

始めに、共通鍵取得部15γが、暗号化復号化装置10γの外部からの入力により共通鍵を取得するかまたは共通鍵の生成を行なう（ステップS301γ）。

それから共通鍵暗号化部16γは、ネットワークを介して予め取得している利用者の公開鍵を利用して共通鍵を暗号化した暗号化鍵を生成する（ステップS302γ）。

さらに、共通鍵改竄検出情報作成部17γは、共通鍵作成者の秘密鍵等の共通鍵作成者に関する情報を共通鍵改竄検出情報としての鍵情報として作成する（ステップS303γ）。

データ暗号化部21γはデータパーツ1γ（平文）を暗号化し暗号文1

$\gamma$  を生成する (ステップ S 3 0 4  $\gamma$ )。

さらに、データ改竄検出情報作成部 2 2  $\gamma$  は、データパーツ 1  $\gamma$  からデータパーツ 1  $\gamma$  に関する情報であるデータ改竄検出情報 1  $\gamma$  を作成する (ステップ S 3 0 5  $\gamma$ )。なお、データパーツが  $n$  個からなる場合、ステップ S 3 0 4  $\gamma$  からステップ S 3 0 5  $\gamma$  の処理を  $n$  回繰り返す。

そして暗号文 1、2、 $\dots$ 、 $n$ 、データ改竄検出情報 1、2、 $\dots$ 、 $n$ 、鍵情報、暗号化鍵の組を暗号化情報として情報保管装置 3 0  $\gamma$  へ送信する (ステップ S 3 0 6  $\gamma$ )。

なお、上記説明は利用者が 1 人で、使用する暗号化鍵が 1 種類の場合である。暗号化情報を共有する利用者が複数 (例えば  $m$  人) である場合は、ステップ S 3 0 2  $\gamma$  で、各利用者毎の公開鍵を用いて  $m$  種の暗号化鍵を生成させる。すなわち、利用者毎に対応する暗号化鍵が生成されることになる。

図 2 2 に、暗号化前の情報の構成と、暗号化された暗号化情報の構成を示す。ここでは、暗号化前のデータパーツ 1、2、 $\dots$ 、 $n$  から、暗号化情報として、暗号文 1、2、 $\dots$ 、 $n$  とデータ改竄検出情報 1、2、 $\dots$ 、 $n$  と暗号化鍵 1、2、 $\dots$ 、 $m$  と鍵情報が作成されることを示している。

次に、複数 ( $n$  個) のデータパーツの暗号文を含む暗号化情報を復号化する際の暗号化復号化装置 1 0  $\gamma$  の動作を図 2 3 の動作フローチャートを参照して説明する。

なおこの処理は、暗号化鍵を作成する際に用いた公開鍵と対をなす秘密鍵を所有する者が行なえるものである。

まず、暗号化復号化装置 10 γ は情報保管装置 30 γ に記憶されている暗号化情報を取得する（ステップ S 501 γ）。なお、暗号化情報に含まれる暗号化鍵は、ユーザ名やユーザ ID 等により対応づけられ、利用者に対応した暗号化鍵が情報保管装置 30 γ から暗号化復号化装置 10 γ に送られるものとする。

そして共通鍵復号化部 18 γ は、利用者の秘密鍵を用いて暗号化鍵を復号化し共通鍵を得る（ステップ S 502 γ）。ここで利用者の秘密鍵は、予め入力されているものとする。

次に、共通鍵改竄検出情報作成部 19 γ は、ステップ S 502 γ で得た共通鍵から共通鍵改竄検出情報を作成する（ステップ S 503 γ）。

そして改竄検証部 20 γ は、取得した鍵情報と共通鍵改竄検出情報を比較検証し鍵作成者の正当性を検証する（ステップ S 504 γ）。この場合、2つの情報が一致することで鍵作成者の正当性を判断できる。

ステップ S 504 γ で、鍵作成者が正当であると判断された場合、n 個の暗号文と n 個のデータ改竄検出情報の組を順に以下の処理を行なう。

まず、データ復号化部 23 γ は暗号文を共通鍵を用いて復号化する（ステップ S 505 γ）。

そして、データ改竄検出情報作成部 24 γ は、復号化したデータパーツを用いてデータ改竄検出情報を作成する（ステップ S 506 γ）。なお、ここで作成したデータ改竄検出情報を第 1 データ改竄検出情報と呼び、暗

号化情報として保持されているデータ改竄検出情報を第2データ改竄検出情報と呼ぶことにする。

次に改竄検証部25γは、作成された第1データ改竄検出情報と暗号化情報の一部である第2データ改竄検出情報を比較し改竄が行われていないか検証する（ステップS507γ）。2つの情報が一致することで改竄が行われていないことが検証される。

ステップS507γで、改竄がないと判断されれば復号化したデータパーツ（平文）を出力する（ステップS508γ）。

なお、以上の説明では、ユーザ名やユーザID等と暗号化鍵を対応づけることで、鍵復号化部12γが利用者に対応する暗号化鍵のみを用いるようにしている。複数の暗号化鍵がある（すなわち、暗号化情報を共有する利用者が複数存在する）場合、利用者に対応する暗号化鍵を得るその他の方法として、上記ステップS502γ～S504γを以下のようにする。まず、ステップS502γにおいてすべての暗号化鍵を復号化する。ステップS502γで複数の暗号化鍵を復号化した場合、正式でないものも含めて複数の共通鍵が生成される。ステップS503γでは、ステップS502γで生成されたすべての共通鍵に対し共通鍵改竄検出情報を作成する。次に、ステップS504γで、各共通鍵改竄検出情報と鍵情報とを比較検証する。すべての組み合わせが異なるとき改竄が行われていることがわかり、一致するものがあれば対応する共通鍵が正式の共通鍵であることがわかる。

次に、上述した、データパーツ1、2、…、nから暗号化情報を作成し

情報保管装置 30 γ に転送した段階から、ここではさらに上記の暗号化情報に情報を追加する際の暗号化復号化装置 10 γ の動作を図 24 に示す動作フローチャートを参照して説明する。

まず、暗号化情報が保管されている情報保管装置 30 γ から暗号化鍵と鍵情報を取得する（ステップ S 601 γ）。なお、暗号化情報に含まれる暗号化鍵は、ユーザ名やユーザ ID 等により対応づけられ、利用者に対応した暗号化鍵が情報保管装置 30 γ から暗号化復号化装置 10 γ に送られるものとする。

そして、共通鍵復号化部 18 γ は、利用者の秘密鍵を用いて利用者に対応する暗号化鍵を復号化する（ステップ S 602 γ）。ここで利用者の秘密鍵は、予め入力されているものとする。

次に、共通鍵改竄検出情報作成部 19 γ は、ステップ S 602 γ で得た共通鍵から共通鍵改竄検出情報を作成する（ステップ S 603 γ）。

改竄検証部 20 γ は、先の鍵情報と共通鍵改竄検出情報が一致するか比較検証し、鍵作成者の正当性を検証する（ステップ S 604 γ）。この場合、2つの情報が一致することで鍵作成者の正当性を判断できる。

ステップ S 604 γ で、鍵作成者が正当であると判断された場合、データ暗号化部 21 γ は追加するデータパーツ  $n+1$  を暗号化し暗号文  $n+1$  を生成する（ステップ S 605 γ）。

さらにデータ改竄検出情報作成部 22 γ はデータパーツ  $n+1$  から改竄

検出情報  $n + 1$  を作成する (ステップ S 6 0 6  $\gamma$ )。

なお、追加するデータパーツが  $L$  個からなる場合、ステップ S 6 0 5  $\gamma$  からステップ S 6 0 6  $\gamma$  の処理を  $L$  回繰り返す。

そして暗号文  $n + 1$ 、 $n + 2$ 、 $\dots$ 、 $n + L$  と改竄検出情報  $n + 1$ 、 $n + 2$ 、 $\dots$

、 $n + L$  を情報保管装置 3 0  $\gamma$  に転送し暗号化情報として追加保管する (ステップ S 6 0 7  $\gamma$ )。

なお、以上の説明では、ユーザ名やユーザ ID 等と暗号化鍵を対応づけることで、鍵復号化部 1 2  $\gamma$  が利用者に対応する暗号化鍵のみを用いるようにしている。複数の暗号化鍵がある (すなわち、暗号化情報を共有する利用者が複数存在する) 場合、利用者に対応する暗号化鍵を得るその他の方法として、上記ステップ S 6 0 2  $\gamma$  ~ S 6 0 4  $\gamma$  を以下のようにする。まず、ステップ S 6 0 2  $\gamma$  においてすべての暗号化鍵を復号化する。ステップ S 6 0 2  $\gamma$  で複数の暗号化鍵を復号化した場合、正式でないものも含めて複数の共通鍵が生成される。ステップ S 6 0 3  $\gamma$  では、ステップ S 6 0 2  $\gamma$  で生成されたすべての共通鍵に対し共通鍵改竄検出情報を作成する。次に、ステップ S 6 0 4  $\gamma$  で、各共通鍵改竄検出情報と鍵情報とを比較検証する。すべての組み合わせが異なるとき改竄が行われていることがわかり、一致するものがあれば対応する共通鍵が正式の共通鍵であることがわかる。

図 2 5 に、暗号化情報の追加前の構成と、追加後の構成を示す。ここでは、暗号化情報として、暗号文  $n + 1$ 、 $n + 2$ 、 $\dots$ 、 $n + L$  とデータ改竄検出情報  $n + 1$ 、 $n + 2$ 、 $\dots$ 、 $n + L$  がもとの暗号化情報に追加されていることを示している。



次に、情報保管装置 30 γ に記憶されている暗号化情報を共有しているチームに、共有メンバーを追加する際の暗号化復号化装置 10 γ の動作を図 26 に示す動作フローチャートを参照して説明する。ここでは、共有メンバー A、B が所属しているチームに、共有メンバー B が、新しい共有メンバーとして共有メンバー C を追加する場合を説明する。

まず、共有メンバー B の操作により、暗号化復号化装置 10 γ は情報保管装置 30 γ にアクセスし、鍵情報と共有メンバー B に対応する暗号化鍵 B を取得する（ステップ S 801 γ）。

共通鍵復号化部 18 γ は、受信者である共有メンバー B の秘密鍵を用いて暗号化鍵 B を復号化し、共通鍵を得る（ステップ S 802 γ）。

共通鍵改竄検出情報作成部 19 γ は共通鍵から共通鍵改竄検出情報を作成する（ステップ S 803 γ）。

そして改竄検証部 20 γ は、取得した鍵情報と共通鍵改竄検出情報を比較検証し鍵作成者の正当性を確認する（ステップ S 804 γ）。この場合、2 つの情報が一致することで改竄が行われていないことが検証される。

ステップ S 804 γ で、鍵作成者の正当性が確認されると、共通鍵暗号化部 16 γ は共有メンバーとして追加する共有メンバー C の公開鍵を用いて共通鍵を暗号化し、暗号化鍵 C を生成する（ステップ S 805 γ）。

鍵暗号化部 12 γ は生成された暗号化鍵 C を情報保管装置 30 γ へ転送

する（ステップS 8 0 6 γ）。

こうして、情報保管装置 3 0 γには3人の共有メンバーに対応する暗号化鍵A、B、Cが保管されることになり、以後、追加された共有メンバーCは、チームの暗号化情報に対する参照・変更等を行なえるようになる。

図 2 7 に、共有メンバーCの追加前の暗号化情報の構成と、追加後の構成を示す。ここでは、暗号化情報として、あらたな共有メンバーである共有メンバーC用の暗号化鍵Cがもとの暗号化情報に追加されていることを示している。

次に、共有メンバーを削除する際の暗号化復号化装置 1 0 γの動作を図 2 8 に示す動作フローチャートを参照して説明する。ここでは、共有メンバーA、B、Cが所属しているチームにおいて、共有メンバーBが共有メンバーAを削除する場合を説明する。

暗号化復号化装置 1 0 γは、共有メンバーBの入力操作による共有メンバーAを削除するための削除命令を取得する（ステップS 1 0 1 γ）。

データ改竄検出情報作成部 2 2 γは、共有メンバーAの削除命令に対応するデータ改竄検出情報を作成する（ステップS 1 0 2 γ）。

次に、暗号化復号化装置 1 0 γは、共有メンバーの削除命令と、削除命令を出した本人を識別する識別情報となるデータ改竄検出情報の組からなる削除情報を情報保管装置 3 0 γに転送する（ステップS 1 0 3 γ）。

なお、情報保管装置 3 0 γは、削除命令を出した本人を識別する機能を

もち、削除命令に応じた暗号化鍵を削除できるものとする。また、ここで用いるデータ改竄検出情報として、共有メンバーAの削除命令に対する共有メンバーBのデジタル署名を用いてもよい。また、削除命令を出した本人を識別する識別情報としてID、パスワード等を用い情報保管装置30γが、情報保管装置30γに登録されている識別情報とを照合するようにしてもよい。

図29に、共有メンバーAの削除前の暗号化情報の構成と、削除後の構成を示す。ここでは、暗号化情報として、共有メンバーA用の暗号化鍵Aがもとの暗号化情報から削除されていることを示している。

次に本実施形態の暗号化復号化装置10γの動作を具体例をあげて詳細に説明する。

まず第3-1の実施例として、ユーザBが、チーム101γ（ユーザA、B、Cの3人が所属）で共有しているスケジュールの1998年の10月1日の項目に用件「セミナー参加」と「15:00」を加える際の処理を説明する。なお本実施例では、スケジュールに関する情報は暗号化情報と暗号化されていない情報を含み

、外部の情報保管装置30γに保管されているものとする。また情報保管装置30γは、ユーザのアクセス権に応じて保管されている情報に対するアクセスを制限できるものとする。また、ユーザBが使用する暗号化復号化装置10γは、ユーザBによるデータの入力を受け付ける入力部（図示せず）と、情報を表示する表示部（図示せず）を備えているものとする。

まず、ユーザBは暗号化復号化装置10γから情報保管装置30γにアクセスし、チーム101γの1998年10月のスケジュールにアクセスできるか確認する。

アクセス可能である場合、チーム101γの1998年10月のスケジュールにアクセスする。情報保管装置30γは、チーム101γの1998年10月のスケジュールを暗号化復号化装置10γに転送し、暗号化復号化装置10γはその表示部にスケジュールを表示する。なお、この段階ではスケジュールの情報はまだ暗号化されていないものとする。

ユーザBは、暗号化復号化装置10γの入力部を用いて1998年の10月1日の項目に「セミナー参加」と「15:00～」を入力する。

次に、共通鍵暗号化部16γにおいて共通鍵を生成する。本実施例ではこの共通鍵をcKey1γと呼ぶことにする。

次に、共通鍵暗号化部16γで、ユーザA、ユーザB、ユーザCの公開鍵を利用して、例えば公開鍵暗号方式であるRSA方式で暗号化する。こうして共通鍵暗号化部では、3人のユーザに対応して3つの暗号化鍵が生成される。本実施例ではこれらの暗号化鍵をそれぞれ、eKey1Aγ、eKey1Bγ、eKey1Cγと呼ぶことにする。

次に、共通鍵改竄検出情報作成部17γは、共通鍵のメッセージダイジェストであるMDγを作成し、さらにこのMDγにユーザBの秘密鍵を利用してデジタル署名を行なう。このデジタル署名を行なったMDγが鍵情報であるSignedKey1γである。

データ暗号化部21γは、スケジュールのデータパーツである「セミナー参加」を共通鍵cKey1γで暗号化を行ない、暗号文CryptDa

t a l γ を生成する。

次に、データ改竄検出情報作成部 2 2 γ は、一例としてハッシュ関数である MD 5 を利用して「セミナー参加」のメッセージダイジェスト M e s s a g e D 1 γ を生成する。

「セミナー参加」に適用した手順をスケジュールのデータパーツである「1 5 : 0 0 ~」に対して行ない、「1 5 : 0 0 ~」の暗号文 C r y p t D a t a 2 γ とメッセージダイジェスト M e s s a g e D 2 γ を得る。

そしてこれらの情報を暗号化復号化装置 1 0 γ から情報保管装置 3 0 γ に転送する。

なお、このときの情報保管装置 3 0 γ に記憶される情報の構成を図 3 0 に示す。上記処理で作成されたスケジュールを区別する情報、ユーザ I D と暗号化鍵、鍵情報、暗号文とデータ改竄検出情報および関連情報が記憶される。

次に第 3 - 2 の実施例として、第 3 - 1 の実施例からさらに、第 3 - 1 の実施例で作成された暗号化情報にユーザ A が、チーム 1 0 1 γ (ユーザ A、B、C の 3 人が所属) で共有しているスケジュールの 1 9 9 8 年の 1 0 月 2 日の項目に用件「会議」と「1 7 : 0 0 ~」を加える際の処理を説明する。

まず、ユーザ A は暗号化復号化装置 1 0 γ から情報保管装置 3 0 γ にアクセスし、チーム 1 0 1 γ の 1 9 9 8 年 1 0 月のスケジュールにアクセスできるか確認する。

アクセス可能である場合、チーム101の1998年10月のスケジュールにアクセスする。情報保管装置30γは、暗号化鍵eKey1Aγと鍵情報SignedKey1γを暗号化復号化装置10γに転送する。

ユーザAは、暗号化復号化装置10γの入力部を用いて1998年の10月2日の用件項目に「会議」と「17:00～」を入力する。

次に、共通鍵復号化部18γは、ユーザAの秘密鍵を用いて暗号化鍵eKey1Aγを復号化し共通鍵cKey1γを生成する。

次に、共通鍵改竄検出情報作成部19γは、共通鍵cKey1γのメッセージダイジェストkeyD1'γを作成する。

次に、改竄検証部20γは、鍵情報のSignedKey1γをユーザBの公開鍵を利用して復号化し、暗号化前の共通鍵のメッセージダイジェストkeyD1γを得る。そして、keyD1γとkeyD1'γを比較する。keyD1γとkeyD1'γが等しければ、チーム101γに所属するユーザBによって作成された共通鍵を改竄されることなく取得できたことがわかる。こうして共通鍵の正当性が確認できる。ここで、ユーザBが共通鍵を作成することが正当であるかどうか、すなわち、共通鍵作成者自身の正当性確認は、共通鍵作成者正当性確認用情報として取得する必要がある。この場合の共通鍵作成者正当性確認用情報の取得方法の一例としては、共通鍵作成者がユーザBであることを暗号化復号化装置10γの表示部にダイアログボックスとして表示し、ユーザに確認してもらう方法をとってもよい。または、ネットワークを介して情報保管装置30γから

関連情報として取得してもよい。

次に、データ暗号化部 21 γ は、スケジュールのデータパーツである「会議」を共通鍵 c K e y 1 γ で暗号化を行ない、暗号文 C r y p t D a t a 3 γ を生成する。

次に、データ改竄検出情報作成部 22 γ は、一例としてハッシュ関数である MD 5 を利用して「会議」のメッセージダイジェスト M e s s a g e D 3 γ を生成する。

「会議」に適用した手順をスケジュールのデータパーツである「17 : 00 ~」に対して行ない、「17 : 00 ~」の暗号文 C r y p t D a t a 4 γ とメッセージダイジェスト M e s s a g e D 4 γ を得る。

そしてこれらの情報を暗号化復号化装置 10 γ から情報保管装置 30 γ に転送する。

なお、このときの情報保管装置 30 γ に記憶される情報の構成を図 31 に示す。上記処理で暗号文とデータ改竄検出情報が追加されているところを示している。

次に第 3-3 の実施例として、第 3-1、第 3-2 の実施例で作成され情報保管装置 30 γ に保管されているチーム 101 γ の 1998 年 10 月のスケジュールをユーザ C が参照する場合の処理を説明する。

まず、ユーザ C は暗号化復号化装置 10 γ から情報保管装置 30 γ にア

クセスし、チーム101γの1998年10月のスケジュールにアクセスできるか確認する。

アクセス可能である場合、チーム101γの1998年10月のスケジュールにアクセスする。情報保管装置30γは、チーム101γの1998年10月のスケジュールと暗号化鍵eKey1Cγと鍵情報SignedKey1γを暗号化復号化装置に転送する。

共通鍵復号化部18γは、ユーザCの秘密鍵を用いて暗号化鍵eKey1Cγを復号化し共通鍵cKey1γを得る。

次に、共通鍵改竄検出情報作成部19γで、共通鍵cKey1γのメッセージダイジェストcKeyD'γを作成する。

改竄検証部20γでは、SignedKey1γをユーザBの公開鍵を用いて復号化し、暗号化前の共通鍵のメッセージダイジェストcKeyDγを得る。そして、このメッセージダイジェストcKeyDγと先のメッセージダイジェストcKeyD'γを比較する。この2つのメッセージダイジェストが等しければチーム101γに所属するユーザBによって作成された共通鍵cKey1γを改竄されることがなく取得できたことが検証できる。すなわち、取得した共通鍵の正当性を確認することができる。また、ここで共通鍵作成者自身の正当性確認を行なう必要があるが、第3-2の実施例で説明したとおりである。

次に、データ復号化部23γは、暗号文CryptData1γを共通鍵復号化部18γより取得した共通鍵cKey1γを用いて復号化を行な



う。ここで平文「セミナー参加」が得られる。

次に、データ改竄検出情報作成部24γで、ハッシュ関数の1つであるMD5を用いて平文のメッセージダイジェストMessage D1'γを生成する。

情報保管装置30γより転送されてきたメッセージダイジェストMessage D1γとデータ改竄検出情報作成部24γで生成されたメッセージダイジェストMessage D1'γを比較する。これら2つのメッセージダイジェストが等しければチーム101γに所属する者によって作成されたデータパーツを改竄されることなく取得できたことがわかる。

同様の手順を繰り返すことで暗号文Crypt Data 2γ…Crypt Data 4γに対して行なうと、「15:00～」、「会議」、「17:00～」を得ることができる。復号化後のスケジュールの表示例を図32に示す。図に示すようにユーザBが入力したデータパーツ「セミナー参加」、「15:00～」とユーザAが入力したデータパーツ「会議」、「17:00～」を同じチームに所属するユーザCは見ることができる。

以上のように、1つのチームに所属する共有メンバーは、暗号化情報に対するデータパーツの追加や変更、他共有メンバーのデータパーツの参照等、自由に行なえるが、共有メンバー以外の者に対して秘匿性を保つことができる。

また一例として、Message D1γ、…、Message D4γの各サイズを16バイト、鍵情報のサイズを2300バイト（下限がある）

であるとする、本実施例では

$$16 \times 4 + 2300 = 2364 \text{ バイト}$$

がオーバーヘッドとなる。

従来の方式で4つの暗号文のそれぞれにデジタル署名を付ける場合は

$$2300 \times 4 = 9200 \text{ バイト}$$

のオーバーヘッドとなり、本発明の方式が従来方式より情報量を抑えることができる。

なお、第3の実施形態の発明は、インターネットの他、LANやダイヤルアップによるネットワークを利用してもよい。

また、本発明の暗号化装置、復号化装置、及び方法を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより暗号化

、復号化の処理を行ってもよい。

すなわち、暗号化プログラムを記録したコンピュータ読み取り可能な記録媒体において、暗号化プログラムは、共通鍵暗号方式を利用して暗号化に用いる共通鍵を取得または生成する機能と、公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化鍵とする機能と、前記共通鍵より鍵情報を作成する機能と、平文を共通鍵暗号方式を利用して暗号化し暗号文とする機能と、前記平文より第1データ改竄検出情報を作成する機能をコンピュータに実現させる。

また、復号化プログラムを記録したコンピュータ読み取り可能な記録媒体において、復号化プログラムは、公開鍵暗号方式を利用して前記暗号化鍵を復号化する機能と、前記暗号化鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する機能と、前記鍵情報と前記共通鍵改竄検出情報とから

改竄検証する機能と、前記暗号文を共通鍵暗号方式で復号化する機能と、前記暗号文を復号化した平文より第2データ改竄検出情報を作成する機能と、前記第1データ改竄検出情報と前記第2データ改竄検出情報とから改竄検証する機能をコンピュータに実現させる。

以上、詳細に説明したように、第3の実施形態の発明によれば平文毎に改竄検出情報を作成することはせず、各平文を暗号化する共通鍵に対して改竄検出情報となる鍵情報を作成し、改竄検出と共通鍵作成者の本人確認を可能としたので、情報を暗号化した暗号化情報のオーバーヘッドを減少させることができる。したがって、暗号化情報の転送時におけるネットワークにかかる負荷と暗号化情報を保管する際に要する記憶装置の容量を減少させることができる。また、各平文に第1データ改竄検出情報を付加したので、個々の平文毎に改竄検出が可能である。また、利用者毎に暗号化鍵を作成することで複数の利用者間で暗号化情報を共有できる。

第4-1～4-4の実施形態の発明は、複数のユーザ（メンバ）から構成される企業の部や課といったチームを階層化するためのチームデータリストを作成、管理、保管してゆくとともに、ユーザに提供される各種の情報や様々な機能をユーザ間で安全に共有するためのチームデータリスト処理システムに関するものである。さらに詳細には、チームデータリストの保管に係わる処理を担うチームデータリスト保管装置と、チームデータリスト保管装置上から取得したチームデータリストを対象に様々な管理を行うチームデータリスト管理装置を備えたシステムに関するものである。

第4-1～4-4の実施形態の発明に関し、従来以下説明する技術が知られている。

ユーザに提供される各種の機能や情報といった様々な資源を複数のユーザ間で共有するためには、これら資源にアクセスを要求しているユーザが、本当に資源へアクセスする権利を有しているのか否かを検証する機能を用意しておく必要がある。かかる検証を行うために、従来は、資源に対する正当なアクセス権限を付与されたユーザを予め定義したアクセスコントロールリスト（以下、「ACL」と略記する）と呼ばれるリストを利用している。なお、ここで言うACLは、上述したチームデータリストに含まれる種々の情報のうち、共有資源に対するアクセスを制御するための情報だけが含まれたリストの一例である。

図51は、ACLを利用して複数のユーザ間で情報共有を行う従来のシステムの概要を示したものである。同図に示されるシステムでは、イントラネット1δ、インターネット2δがそれぞれファイアウォール3δ、4δを介してサーバ5δに接続されており、イントラネット1δ内部の者ばかりでなく、イントラネット外の共有メンバ6δがインターネット2δを介して互いに情報を共有している。周知のように、イントラネット1は企業内に整備されたネットワークなどの閉じたネットワークであり、その一方で、インターネット2δは世界中にまたがるパブリックなネットワークである。

また、ファイアウォール3δ、4δは悪意を持った侵入者などがイントラネット1δへ不正にアクセスすることを防止するためのコンピュータである。サーバ5δは各種の資源が蓄積されている端末（コンピュータ）であって、共有情報が格納されたデータベース7と、特定の情報ないし機能にアクセスしても良いグループ及びそれに属するメンバのメンバリストを保持したACL8δを備えている。このサーバ5δは、データベース7に

蓄積されている共有情報を管理するデータ保管機能のほか、クライアントに相当する通信相手が予め許可されている者か否かを検証するユーザ認証機能、ACL 8 δに基づいて共有情報に対するアクセスの可否を検証するアクセス制御機能、ACL 8 δに基づいて特定のグループに属するメンバーだけが特定の共有情報へアクセスすることを可能ならしめるグループ管理機能を備えている。

図51のシステムでは、共有メンバーδやイントラネット1 δ内部のユーザからデータベース7 δに対するアクセス要求があると、サーバ5 δはその都度ACL 8 δを参照してユーザ認証を行い、当該ユーザがメンバーとしてACL 8 δに定義されていればアクセスを許可し、メンバーとして定義されていなければアクセスを拒否する。また、当該ユーザに対してアクセスが許可されている場合、サーバ5 δはACL 8 δを参照して当該メンバーが特定のグループに含まれるかどうかを確認するとともに、当該メンバーがアクセス要求のある共有情報に関してアクセスを許されているかどうか調べるようにしている。

ところで、複数のユーザ間で資源を共有する場合にはサーバ側の管理者を共有メンバーに含めるのが好ましくない場合もある。例えば、ある企業の情報システム部に所属するシステム管理者は、人事部内だけで共有すべき企業の人事情報にアクセス不可能であることが必要と考えられる。ところが、上述した図51のようなシステムでは、サーバ5 δの管理者に対してACL 8 δの設定や管理を行う権限を許与してしまっている。そのため、サーバ管理者5 δがACL 8 δに対して不正なアクセスを行うことが可能であり、意図的にACL 8 δの設定内容が改竄されるのを防止することができない欠点がある。これに加えて、サーバ管理者以外にも、サーバSV

δへ不正に侵入する者（いわゆるクラッカ）によってACL 8 δが不正に改竄されてしまうおそれもある。

このほか、企業内部で情報を共有してゆく利用形態などへの適用を考えた場合

、そうした形態にうまく適合したシステムを構築してゆくことが望ましい。すなわち、ある程度以上の規模の企業では組織がピラミッド状に形成された階層関係になっており、例えば、人事部の配下には人事一課や人事二課が設置されていることなどはごく一般的であると言える。また、開発部門などでは商品の開発工程などに合わせて例えば開発部長が新たに課を作ったり、幾つかの課を統合したり

、あるいは、ある特定の課を廃止したりする権限が与えられている場合も考えられる。また、それぞれの課が業務別にいくつかのグループに分かれていることもある。

そうした組織にあっては、開発部長が各課やそれぞれの課に属する全てのグループの構成員を管理することは非常な負担である。そこで、こうした管理負担を分散するために、開発部長を補佐する者を何人か割り当てるようにしてこれらの者に管理業務の一部又は全部を代行させることなどが行われている。さらには、開発部長には課の作成、統廃合等の業務を行う権限だけを与えておき、課内部の管理や情報共有自体は課長やその下のグループリーダ等に一任するといった形態が採られている。しかるに、上述した従来のシステムではいま説明したような企業の組織形態に適合した柔軟な管理や情報共有は何ら考慮されていないという問題がある。

本発明は上記の点に鑑みてなされたものであり、その目的は、サーバの

管理者といった特権者も含め、企業の組織単位等に相当するチームの外にいる者、クラッカ等がチームデータリストに不正を行うことを防止しつつ、チームの階層化および各種の情報や機能の実現するためのチームデータリスト処理システムを提供することにある。さらに詳しくは、各チームに所属しているメンバから特に選ばれた者だけが、チームの配下にサブチームを作成したり、サブチームの作成権限を特定の複数人に割り当てたり、サブチームの作成権限者が選定した特定人にサブチーム内の管理を行わせたりすることが可能なチームデータリスト処理システムを提供することにある。

以下、図面を参照して第4-1～4-4の実施形態について説明するが、まず初めに本発明におけるチームデータリストについて説明する。本発明におけるチームデータリストは、チームに関する情報を定義したリストの総称であって、上述したACLのような機密性の高い管理が要求される用途に適用される「メンバの集合」を定義するためのものである。上述した通り、従来のシステムでは、チームのメンバではない端末管理者、ネットワーク管理者、サーバ管理者などがチームに関する情報を変更することができる。一方、本発明におけるチームデータリストでは、チームに関する情報を複数のリスト（後述するようなオーソリティリスト、オーソリティデータやメンバリスト、チームマスタリスト、アプリケーションリスト）に分割して管理することで、チームの階層化やチームマスタ自身の変更といったチーム管理をチーム内のメンバだけで行えるようにしている。

以下に詳述する実施形態では、第一に、チームの配下にサブチームを作成できるようにして、会社組織等における階層関係を模擬して情報共有を行ってゆく仕組みを実現している。第二には、特に選定された複数の人間

に対してサブチームの作成権限を授与できるような仕組みを実現しており、それによって一人の管理者に負荷が集中しないようにして管理負担の分散を図っている。第三には、サブチーム内部の管理については、サブチーム作成権限者がサブチーム内から選んだ特定の者に行わせる仕組みを実現している。そうすることによって、チームの管理者がサブチーム内部の管理や情報共有に関与しなくとも済むようにしている。

#### 〔第4－1 実施形態〕

本実施形態では、階層化されたチームに合わせて、チームデータリストにアクセスできる者をその権限の内容に応じてメンバ、サブオーナー、チームマスタの3種類に分類しており、この順番でその者に付与される権限が拡大してゆく

。チームマスタは或るチームの管理者であって、当該チームの配下の組織たるサブチームの作成といった管理権限を有する者である。一方、サブオーナーはチームマスタによって指名された者であって、チームマスタと同様にサブチームの作成といった管理権限を持つ者であるが、他の者をサブオーナーとして指名することは許されていない。サブオーナーは複数人いる場合もあれば一人もいない場合もある。他方、サブオーナー及びチームマスタ以外の一般のメンバは情報や機能を共有する者であって、サブチームの作成権限などの特権はいつさい与えられていない。なお、サブオーナーやチームマスタは特別な権限が与えられてはいるが、チーム内のメンバであることに変わりはなく、その意味でサブオーナーやチームマスタをメンバと呼ぶこともある。なお、以下の説明及び図面ではチームマスタを「TMδ」と略記し、サブオーナーを「sub AUδ」と略記することがある。



以下、チームデータリスト管理装置及びチームデータリスト保管装置の2つの装置を備えたシステムについて本実施形態を説明してゆく。図37は、チームデータリスト管理装置及びチームデータリスト保管装置を具備した本実施形態のシステム全体の構成を示したブロック図である。同図において、チームデータリスト管理装置30δ、チームデータリスト保管装置31δは以下に詳述するチームデータリスト管理機能、チームデータリスト保管機能をそれぞれ備えており、互いに通信機能を利用してデータを授受している。チームデータリスト管理装置30δ、チームデータリスト保管装置31δは何れもワークステーションなどの一般的なコンピュータで実現することが可能であり、これらコンピュータの主記憶上にはそれぞれチームデータリスト管理機能、チームデータリスト保管機能を実現するためのプログラム（チームデータリスト管理プログラム、チームデータリスト保管プログラム）が記憶される。

これらのプログラムはフロッピーディスク、IC（集積回路）カード、光磁気ディスク、CD-ROM（コンパクトディスクー読み取り専用メモリ）等の可搬性のある記憶媒体や、コンピュータに内蔵されるハードディスクなどの大容量の記憶媒体といったコンピュータ読み取り可能な記憶媒体にその一部又は全部が記憶されている。すなわち、当該プログラムは以下に詳述する機能の一部を実現するためのものであっても良く、さらにはコンピュータにすでに記録されているプログラムとの組み合わせでこれら機能を実現できるものであっても良い。そして

、チームデータリスト管理装置やチームデータリスト保管装置を作動させるにあたって、これらのプログラムがコンピュータ上のCPU（中央処理装置）の指示の下に予め記憶媒体から主記憶上に転送される。その後、CPUは主記憶上に転送されたプログラムを実行し、それによって装置各部

を制御して、以下に詳述する様々な処理を実現している。

なお、ここで言う「コンピュータ」にはOS（オペレーティングシステム）や周辺機器等のハードウェアが含まれている。また、コンピュータ読み取り可能な記憶媒体としてはいま述べたようなプログラムを静的に記憶するものに限られるものではなく、専用線や電話回線などの通信回線を通じて短時間だけ動的にプログラムを保持するもの、即ち、インターネット等のネットワークでプログラムやデータを保持、転送、中継するサーバ、ルータ、ゲートウェイといったコンピュータ機器に内蔵された主記憶やキャッシュメモリ、サーバ、クライアントとして機能するコンピュータ内部の揮発性メモリなどのように、一定時間プログラムを保持可能なものをすべて包含している。

さて、図37に示すチームデータリスト保管装置31δにはハードディスク等のデータベースを構築可能な記憶装置32δが接続されている。この記憶装置32δは、複数のメンバで構成されるチーム毎にオーソリティデータ33δとオーソリティリスト34δからなるチームデータリストの組を記憶している。同図では説明の都合からオーソリティデータ33δ及びオーソリティリスト34δの組を一つだけ示しているが、実際にはチームの数だけこれらの組が存在している。ここで、図38A、Bはオーソリティデータ33δ、オーソリティリスト34δの詳細な構造を示したものである。また、図38C、38Dはこれ以後に掲げる図面中において、オーソリティデータ33δ、オーソリティリスト34δの記憶内容を簡略化して示すための表記法をそれぞれ示したものである。なお、以下の説明及び図面ではオーソリティデータを「AUDδ」と略記し、オーソリティリストを「AULδ」と略記することがある。

オーソリティデータ 3 3 δ は或るチームとその配下のサブチームとの関係を表すデータであって、サブチームとの関係において上位にある当該チームを親チームと呼ぶ。図 3 8 A に示すように記号 “A U D δ” がオーソリティデータであることを示しており、このオーソリティデータ 3 3 δ は、自身のチームに付与された識別子たるチーム I D 3 3 a δ、このチームの親チームに付与されたチーム I D である親チーム I D 3 3 b δ、親チームの誰がこのチームを作成したかを意味するチーム作成者 3 3 c δ、このチームに属するメンバの誰に対してチームマスタ権限を与えたかを示すチームマスタ 3 3 d δ、チーム作成者 3 3 c δ のデジタル署名がなされるデジタル署名 3 3 e δ を含んでいる。また、図 3 8 C において、このオーソリティデータはチーム 1 0 1 δ のサブチームであるチーム 1 0 2 δ に関するものであることが分かる。これに加えて、デジタル署名からこのオーソリティデータのチーム作成者がメンバ B δ であることが分かるほか、チームマスタがメンバ X δ であることが分かる。

一方、オーソリティリスト 3 4 δ は各チームにおける複数の管理者を登録したリストであって、当該チームのチームマスタやサブオーソリティに関するデータが含まれている。図 3 8 B に示すように記号 “A U L δ” がオーソリティリストを意味しており、このオーソリティリスト 3 4 δ はこのチームに関するチーム I D 3 4 a δ、チームマスタ 3 4 b δ、サブオーソリティ 3 4 c δ（同図の場合は二人）、チームマスタ 3 4 b δ のデジタル署名であるデジタル署名 3 4 d δ を含んでいる。そして、図 3 8 D によれば、チームマスタがメンバ X δ であってそのデジタル署名がなされているほか、サブオーソリティがメンバ C δ 及びメンバ D δ であることが分かる。なお、図 3 8 D ではチーム I D の表記自体は省略されている。以上の

ように、本実施形態によるチームデータリストは、親チーム及びサブチームの関係を示すリストであるAUD $\delta$ と、サブチーム管理に関わるリストであるAUL $\delta$ に分割された構造となっている。

なお、オーソリティデータ33 $\delta$ やオーソリティリスト34 $\delta$ には、図38A、38B、38C、38Dに示した以外にも、これらデータやリストの作成時間を示すタイムスタンプ、デジタル署名33e $\delta$ やデジタル署名34d $\delta$ を作成するのに用いられるデジタル署名アルゴリズム、オーソリティデータ33 $\delta$ やオーソリティリスト34 $\delta$ 自身の有効期限、オーソリティデータ33 $\delta$ やオーソリティリスト34 $\delta$ 自身の識別番号に関するデータなどを含んでいる。また、メンバ、サブオーソリティ、チームマスタの各個人を識別するためのID（識別子）としては、名前、メールアドレス、組織上の名称、個人のシリアルナンバ、デジタル証明書等、種々のものを用いることが可能である。

次に、図39は階層化されたチームの概念図についてその一例を示したものである。同図に示されるように、チームの階層はコンピュータのファイルシステムのように木構造になっており、図中の楕円形がチームを表現するとともに、親チームとそのサブチームが直線で互いに結ばれている。各チームには複数のサブチームを登録することができ、例えば人事部のチームの配下に人事一課、人事二課などのサブチームを登録することが可能になっている。また、頂点に存在するチーム101 $\delta$ は木構造の根に相当しているため、ファイルシステム上のルートディレクトリになぞらえて本実施形態では「ルート(Root $\delta$ )」ないしルートチームと呼んでいる。さらに、チーム102 $\delta$ 及びチーム103 $\delta$ は何れもチーム101 $\delta$ のサブチームであって、木の上では同じ階層に属するチームである。一方、チ

ーム 1 0 4  $\delta$  はチーム 1 0 3  $\delta$  のサブチームである。

一方、図 4 0 は図 3 9 に示したチーム階層に対応させて各チームのオーソリティリストやオーソリティデータについて具体的な値を記入したものである。なお、同図ではオーソリティリスト及びオーソリティデータの他に、互いに情報や機能を共有する共有メンバの一覧を示したメンバリスト（図中の「ML  $\delta$ 」）が各チームに含まれている例を示してある。つまり、この図においては、チームデータリストがオーソリティリスト、オーソリティデータ、メンバリストの 3 種類のリストで構成される。各メンバリスト 1 0 1 m  $\delta$  ~ 1 0 4 m  $\delta$  にはメンバリストの作成者のデジタル署名とメンバの一覧が図示されているが、これ以外にも、チームの利用目的に合致した様々なチームの管理情報が含まれている。すなわち、各メンバの識別情報、各メンバに付与された公開鍵方式における公開鍵（即ち、所定長のビット列）とこの公開鍵に対応する保有者の識別子（以下、「公開鍵 ID」という）、チーム ID、メンバリストの作成時間を示すタイムスタンプ、チーム内のメンバが利用できる機能（例えば、アプリケーション）に関する情報などが含まれている。このほか、それぞれのメンバリストには各メンバに関する情報として、e-mail（電子メール）アドレスやメンバ自身の住所といった情報も含まれており、これらを用いることで各メンバに関する情報リソースの管理も同時に行うことができる。

同図に示す構成によれば、オーソリティデータに記述された親チーム ID を辿ってゆくことで、何れのサブチームからもルートたるチーム 1 0 1  $\delta$  に到達することができる。このほか、各チームでは複数の管理者がサブチームを作成可能である。例えばチーム 1 0 1  $\delta$  ではチームマスタ A 及びサブオーソリティ B、C がサブチームの作成権限を有しており、オーソリ

ティデータ 102 d δ, 103 d δ のデジタル署名から分かるように、サブチームたるチーム 102 δ, 103 δ はそれぞれチーム 101 δ のサブオーソリティ B, C が作成している。

あるサブチームのオーソリティデータは当該サブチームの親チームに登録された管理者が作成することになっている。また、当該サブチーム内の誰もが親チームの管理者の指示によってこのサブチームのチームマスタになることができる。例えばチーム 104 δ では、オーソリティデータ 104 d δ のデジタル署名がメンバ V であるから、親であるチーム 103 δ の管理者の一人であるサブオーソリティ V がオーソリティデータ 104 d δ を作成しており、チーム 104 δ のチームマスタとしてメンバ L を指名している。

一方、オーソリティリストは各チームのチームマスタが作成してデジタル署名することになっている。例えば、チーム 103 δ のオーソリティリスト 103 u δ はチームマスタたるメンバ X δ が作成したものであって、そこにはメンバ X δ のデジタル署名がなされている。そのため、オーソリティリスト 103 u δ 中のサブオーソリティに関するデータはメンバ X のみが管理できることになり、親チームたるチーム 101 δ の管理者（即ち、チームマスタ A やサブオーソリティ B, C）の干渉を受けることはない。換言するならば、オーソリティリストのデジタル署名者をチームの作成者（即ち、親チームのチームマスタやサブオーソリティ）にしてしまうと、例えば人事部長が人事課長に課内部の管理を任せることができなくなって自分で管理してゆかねばならなくなる。同様にして、メンバリストのデジタル署名についても各チームのチームマスタが行うことから、各チーム内の共有メンバに関する管理についても親チームの干渉を受けずに済むこと

になる。例えばチーム103δのメンバリスト103mδはチームマスタXがデジタル署名しているため、親チームの管理者が管理することはできない。ただし、サブチームを最初に作成したときの初期状態や、サブチームのチームマスタを親チームのチームマスタやサブオーソリティが変更した場合には、オーソリティリストのデジタル署名は、該サブチームを作成した親チームのチームマスタ又はサブオーソリティのデジタル署名となっている。

以上の点をまとめると、本実施形態ではオーソリティデータとオーソリティリストを分離する構成としており、親チームはサブチームのオーソリティデータAUDδを参照することができる一方、親チームの管理者がオーソリティリストやメンバリストを改竄できないようにすることで、サブチーム内部の管理に親チームは関与しないようにしている。これによって、各チームのチームマスタは、自分でサブオーソリティを選択できるほか、チーム内の情報共有のメンバ管理も行うことができる。

次に、図37のチームデータリスト保管装置31δにおいて、権限確認機能35δはクライアントCLδ側からオーソリティデータ33δやオーソリティリスト34δに対する参照、変更、削除の各要求があったときに、要求者を識別してこれらの要求を許可するのか拒否するのかを判断する。この判断にあたっては、要求対象となっているチームのチームマスタ、サブオーソリティや当該チームの親チームやサブチームとの間の関係のほか、チームに所属するメンバ等の権限と要求者本人に与えられている権限などを照らし合わせている。つまり、要求内容によって判断手順の詳細が異なるためその詳細については後述する動作説明に譲る。次に、リスト保管機能36δは権限確認機能35δがオーソリティデータ33δやオーソリテ

ィリスト 3 4 δ を使用するにあたって、これらのリストを記憶装置 3 2 δ から取得し、記憶装置 3 2 δ から削除し、あるいは記憶装置 3 2 δ へ保存する処理を司っている。以下の説明では、権限確認機能 3 5 δ がオーソリティデータ 3 3 δ やオーソリティリスト 3 4 δ にアクセスする場合には必ずリスト保管機能 3 6 δ が介在することを前提としているが、煩雑になるため一々説明しない。

次に、チームデータリスト管理装置 3 0 δ において、リスト正当性確認機能 3 7 δ はルートチームに至るまで親チームのオーソリティリスト及びオーソリティデータを順次辿ってゆき、最終的にチーム 1 0 1 δ のチームマスタ A のデジタル署名を確認してオーソリティリスト及びオーソリティデータの正当性を検証している。なお、ここで言う正当性とは改竄や越権行為などが無く正当な手順を経てチーム階層の管理が行われていることを意味している。次に、AUD・AUL 変更機能 3 8 δ は、リスト正当性確認機能 3 7 δ が取得したオーソリティデータ 3 3 δ やオーソリティリスト 3 4 δ に対してメンバや管理者の追加、削除、置換などの変更を加えるほか、サブチーム作成時などではオーソリティデータ 3 3 δ 及びオーソリティリスト 3 4 δ を新たに作成することもある。次いで、デジタル署名機能 3 9 δ は AUD・AUL 変更機能 3 8 δ によって処理がなされたオーソリティデータ 3 3 δ やオーソリティリスト 3 4 δ に対し、変更者本人しか知り得ない秘密鍵ないしデジタル署名鍵を用いた暗号とハッシュ関数とを併用してこれらリストの作成者ないしは変更者（即ち、チームマスタ又はサブオーソリティ）のデジタル署名を付加する。

次に、公開鍵管理機能 4 0 δ は、チームデータリスト管理装置 3 0 δ に接続された公開鍵データベース 4 1 δ にアクセスして、公開鍵と当該公開



鍵に対応する公開鍵IDを取得する。ちなみに、実際の形態において、公開鍵データベース41δはチームデータリスト管理装置30δに直接的に接続されたローカルな形態のみならず、インターネット等のネットワーク上に設置されたサーバ（例えば、認証局）に存在している形態も当然に考えられる。こうした形態によれば、公開鍵管理機能40δは認証局上に登録されたホームページを介して公開鍵データベース41δにアクセスし、そこから上述した公開鍵及び公開鍵IDをファイルの形式で取得することも可能となる。

次に、上記構成によるチームデータリスト管理装置30δおよびチームデータリスト保管装置31δを有するシステムの動作についてクライアントCLδからサーバSVδに対して為される要求内容毎に説明してゆく。

#### 〔サブチームの作成〕

図41はサブチームを作成するための処理手順を示している。ここでは図40に示したチーム101δのサブオーソリティであるメンバCが、チーム101δの配下にチームマスタをメンバXとしたサブチーム103δを作成するものとする。これは、人事部長の代行として部長代理が人事部の下に課を新設する業務を遂行する場合などに相当する。ここで、チームデータリスト保管装置31δでは正当な手順に従って作成されたチーム101δに関するチームデータリストが予め記憶装置32δ上に格納されており、ルートチーム101δのチームマスタAによる管理体系でサブチームの作成が行われる。なお、図40に示したように、チーム101δには親チームは存在しないのでオーソリティデータ101dδの親チームIDには固定値「Rootδ」が設定されているほか、チームマスタはメンバAであるためオーソリティデータ101dδ及びオーソリティリスト10

101δには何れもメンバAのデジタル署名がされている。もつとも、ルートチームには仮想的に「Rootδ」という親チームがあると見なすことができ、また、この親チームがチームマスタとしてメンバAを指名しているから見なすことができる。

まず、メンバCδからのサブチーム作成指示に従って、チームデータリスト管理装置30δがサブチーム作成要求をチームデータリスト保管装置31δに送出する（ステップS11δ）。チームデータリスト保管装置31δは記憶装置32δからオーソリティデータ101dδ及びオーソリティリスト101uδを取得して、これらをチームデータリスト管理装置30δに送出する。その際、チームデータリスト保管装置31δはチーム101δの配下にサブチーム（即ち、図40に示すチーム102δ）があればそれらチームに関するチームデータリストも併せてチームデータリスト管理装置30δへ送出する（ステップS12δ）。チームデータリスト管理装置30δでは、AUD・AUL変更機能38δがメンバCδからの指示に基づいて、親チームIDをチーム101δ、チームIDをチーム103δ、チームマスタをメンバXとしたオーソリティデータ103dδを作成するとともに、チームマスタをメンバXとしたオーソリティリスト103uaδを作成する。次に、AUD・AUL変更機能38δは作成したオーソリティリスト103uaδをオーソリティデータ103dδと一緒にしてデジタル署名機能39δに引き渡す。

デジタル署名機能39δは、秘密鍵ファイルや秘密鍵の記録されたICカード等からメンバCに関する秘密鍵を取得し、これを基にAUD・AUL変更機能38δから送られたオーソリティデータ103dδ及びオーソリティリスト103uaδに対して要求者たるメンバCのデジタル署名を

行う。この時点ではオーソリティリスト 103 u a δ のデジタル署名はチームマスタ X のものではなく、サブチーム作成者のデジタル署名になっている（以上、ステップ S 13 δ）。次に、デジタル署名機能 39 δ は、チーム 103 δ について作成されたオーソリティデータ 103 d δ 及びオーソリティリスト 103 u a δ をチームデータリスト保管装置 31 δ に送出して、これらの保存要求を行う（ステップ S 14 δ）。

チームデータリスト保管装置 31 δ では、権限確認機能 35 δ が図 42 のフローチャートに示される権限確認を行う。まず、権限確認機能 35 δ は保存要求を行った要求者がメンバ C であることを識別（ステップ S 31 δ）し、チーム 101 δ に関するオーソリティデータ 101 d δ 及びオーソリティリスト 101 u δ を基に、メンバ C がチーム 101 δ のチームマスタ又はサブオーソリティであるかどうか調べる（ステップ S 32 δ）。この場合、メンバ C はチーム 101 δ のサブオーソリティであるため、正当な権限を持つ者によって作成されたデータの保存要求と判断（同ステップの判断結果が“YES”）する。ちなみに、同ステップの判断結果が“NO”となる場合には改竄ないしは不正行為が存在しているため、権限確認機能 35 δ は要求された保存動作を行うことなく処理を中止する。

次に、権限確認機能 35 δ は作成されたサブチーム 103 δ のオーソリティデータ 103 d δ 及びオーソリティリスト 103 u a δ のデジタル署名がともに要求者たるメンバ C のものであることを確認する（ステップ S 33 δ）。この場合は、前述したように何れもメンバ C がデジタル署名しているため同ステップの判断結果は“YES”となり、権限確認機能 35 δ は正常な権限でサブチームが作成されたものと最終的に判断して、作成されたサブチームのオーソリティデータ 103 d δ とオーソリティリスト

103uaδを記憶装置32δに保存する（ステップS34δ）。ちなみに、ステップS33δの判断結果が“NO”となる場合には改竄ないしは不正行為が存在しているため、権限確認機能35δは要求された保存動作を行うことなく処理を中止する（なお、以上の処理は図41のステップS15δに相当）。以上の手順によってサブチームの作成が完了する。

この後、チーム103δのチームマスタたるメンバXから当該チームに対して、情報共有のメンバやサブチーム作成権限者の設定といった管理要求があったものとする。なお、ここでは一事例としてチーム103δのサブオーソリティとしてメンバW及びメンバVを新たに登録する場合について説明する。図41に示すように、まずチームデータリスト管理装置30δは、メンバXから指示された管理要求に基づいて、親チーム103δに関するチームデータリストをチームデータリスト保管装置31δに要求する（ステップS16δ）。すると、チームデータリスト保管装置31δは要求内容をもとにしてサブチーム103δのほかルートチームに至るまでの全ての親チーム（この場合はルートチームたるチーム101δのみ）に関するチームデータリストをそれぞれチームデータリスト管理装置30δ側に転送する（ステップS17δ）。チームデータリスト管理装置30δでは、リスト正当性確認機能37δが図7δのフローチャートに示される処理手順に従って、転送されてきたリストの正当性を調べる（ステップS18δ）。

まず、リスト正当性確認機能37δは、管理対象であるチーム103δのオーソリティデータ103dδ及びオーソリティリスト103uaδのデジタル署名を参照してそれらが改竄されているかどうか確認（ステップS41δ）し、改竄があれば不正行為があったものとして管理要求に関わ

る処理を中止する（同ステップの判断結果が“NO”）。一方、同ステップの判断結果が“YES”であって改竄がなければ、リスト正当性確認機能37δは、オーソリティデータ103dδからメンバXがチーム103δのチームマスタであることを確認できる。ここで、通常であれば、リスト正当性確認機能37δはオーソリティリスト103uaδからそのデジタル署名者がチームマスタたるメンバXであることを確認する。しかし、前述したようにこの時点はサブチーム作成途上の過渡期になっており、オーソリティリスト103uaδのデジタル署名者がサブチーム作成者であるメンバCδになっているので、メンバCがサブチームを作成する正当な権利を持っているかどうかは、後述する処理（ステップS45δ）で、メンバCが親チーム101δのチームマスタもしくはサブオーソリティとして登録されているか調べることで確認する（ステップS42δ）。

次に、リスト正当性確認機能37δはオーソリティデータ103dδの親チームIDから親チームがチーム101δであることを知り（ステップS43δ）、親チームのオーソリティデータ101dδ及びオーソリティリスト101uδのデジタル署名が改竄されているかどうか調べる（ステップS44δ）。そしてこれらの何れかでも改竄されていれば、不正行為があったとしてリスト正当性確認機能37δは処理を中止する（同ステップの判断結果が“NO”）が、同ステップの判断結果が“YES”であって改竄がなければ、引き続いてチーム103δの作成者が親チームのチームマスタ又はサブオーソリティであるかどうかを確認する（ステップS45δ）。この場合、チーム103δのオーソリティデータ103dδのデジタル署名者はメンバCであり、また、親であるチーム101δのオーソリティリスト101uδからメンバCが親チームのサブオーソリティとして登録されていることが分かり、チーム103δが正当な作成権限を持つ

者によって作成されていることが確認できる(同ステップの判断結果が“YES”)。なお、同ステップの判断結果が“NO”であれば、リスト正当性確認機能37δは不正行為があったものとして処理を中止する。

次に、リスト正当性確認機能37δは親であるチーム101δがルートであるかどうか調べるが、この場合はチーム101δのオーソリティデータ101dδの親チームIDが“Rootδ”であることからルートチームであることが分かる(ステップS46δの判断結果が“YES”)。そこで、リスト正当性確認機能37δはチーム101δのオーソリティデータ101dδを調べることでそのチームマスタがメンバAであることが分かる。そして、このメンバAによってオーソリティデータ101dδ及びオーソリティリスト101uδがデジタル署名されていることから、チーム階層がチームマスタAの下で正当に管理されていることを確認できる(ステップS47δ)。最後に、メンバX自身がチームデータリスト管理装置30δを操作して、ルートチーム101δのチームマスタAが管理するチーム階層の下に、情報共有などのチームデータリストの利用や階層化されたチームの利用が為されていることを承認して、この旨をリスト正当性確認機能37δに通知する。

以上の手順により、リスト正当性確認機能37δは、チーム101δのチームマスタAの指名したサブオーソリティCがチーム103δに関するオーソリティデータ及びオーソリティリストを作成しており、チームデータリスト保管装置31δから正常な状態でこれらチームデータリストが取得されていることを確認できる。そこで、リスト正当性確認機能37δはチームデータリスト保管装置31δから転送されたチームデータリストをAUD・AUL変更機能38δに渡す。なお、図43のステップS46δ

で親チームがルートチームと判断されなかった場合、例えばチーム103δのサブチームであるチーム104δに対して管理要求を行った場合、リスト正当性確認機能37δは対象とするチームを親チームに変更してチーム階層をルートチームに向かって一つ上がり（ステップS49δ）、親チームがルートチームたるチーム101δになる（ステップS46δの判断結果が“YES”）までステップS42δ～S46δ及びステップS49δから成るループを繰り返して実行する。

次に、AUD・AUL変更機能38δはチーム103δのオーソリティリスト103uaδに対して、サブオーソリティとしてメンバW及びメンバVを加えたオーソリティリスト103uδを作成し、これをオーソリティデータ103dδとともにデジタル署名機能39δに渡す。デジタル署名機能39δは前述した秘密鍵ファイル等からチームマスタXに関する秘密鍵を取得し、渡されたオーソリティリスト103uδに対してチームマスタXのデジタル署名を行ったのち（以上、ステップS19δ）、これをオーソリティデータ103dδとともにチームデータリスト保管装置31δに転送してこれらチームデータリストに関する保存要求を行う（ステップS20δ）。

チームデータリスト保管装置31δにおいて、権限確認機能35δはチームデータリスト管理装置30δからの保存要求に対し、記憶装置32δに保管されているチーム101δに関わるチームデータリストとクライアント側から転送されてくるチーム103δに関わるチームデータリストに基づいて、図44のフローチャートで示される権限確認を行う。すなわち、まず権限確認機能35δは保存要求を指示した要求者がメンバXであることを識別（ステップS51δ）し、転送されてきたオーソリティデータ1

03dδ及びオーソリティリスト103uδをもとにして、上記要求者が、チーム103δのチームマスタ、親であるチーム101δのチームマスタ又はサブオーソリティの三者のうち何れかに一致するかどうかを確認する。この場合は要求者たるメンバXがチーム103δのチームマスタとして登録されている（ステップS52δの判断結果が“YES”）ので、権限確認機能35δは要求者が保存要求に対する正当な権限を持っていると判断する。ちなみに、同ステップの判断結果が“NO”であれば、権限確認機能35δは要求者に正当な権限が与えられていないものとして処理を中止する。

次に、権限確認機能35δはオーソリティデータ103dδのデジタル署名者が親チームのチームマスタ又はサブオーソリティの何れかに一致するかどうか確認する。この場合、オーソリティデータ103dδのデジタル署名者はメンバCであって親チーム101δのサブオーソリティである（ステップS53δの判断結果が“YES”）ため、権限確認機能35δは要求者が保存要求に対する正当な権限を持っていると判断する。ちなみに、同ステップの判断結果が“NO”であれば、権限確認機能35δは改竄や不正行為があったものとして処理を中止する。次に、権限確認機能35δは、オーソリティリスト103uδのデジタル署名者がオーソリティデータ103dδに登録されているチームマスタと一致するかどうかを確認する。この場合、オーソリティリスト103uδのデジタル署名者はオーソリティデータ103dδの示すチームマスタXである（ステップS54δの判断結果が“YES”）ことから、権限確認機能35δは正常な権限を持つ者によってチーム103δが作成されたものと最終判断を下して、チームデータリスト管理装置30δから転送されたチームデータリストを記憶装置32δに保存して、チーム103δに関するチームデータリスト



の内容を更新する（ステップS 5 5 δ）。なお、ステップS 5 4 δの判断結果が“NO”であったならば、権限確認機能3 5 δは改竄や不正行為があったものとして処理を中止し、上述したステップS 5 5 δにおける保存処理は実施しない。

以上のようにして、サーバS V δ側に保管されているチームデータリストに基づいて、メンバXが間違いなくルートチームのチームマスタAによる管理体系の中で正当にチーム1 0 3 δのチームマスタとして任命されていることが検証できる（図4 1のステップS 2 1 δ）。

#### 〈サブチームのチームマスタの変更〉

次に、サブチームのチームマスタを変更するための処理手順について図4 5を参照して説明する。ここではルートたるチーム1 0 1 δにサブオーソリティとして登録されているメンバBが、サブチームであるチーム1 0 3 δのチームマスタをメンバXからメンバZへ変更する場合を例に挙げることにする。これは人事一課長が異動になったために、人事部長の代わりに部長代理が課長を変更する場合などに相当する。まず、チームデータリスト管理装置3 0 δはサブチーム1 0 3 δに関わるチームデータリストの変更要求をチームデータリスト保管装置3 1 δに送出する（ステップS 6 1 δ）。これにより、チームデータリスト保管装置3 1 δは図4 1のステップS 1 2 δと同様にチーム1 0 1 δとその配下のサブチームに関するチームデータリストをチームデータリスト管理装置3 0 δ側に転送する（ステップS 6 2 δ）。

チームデータリスト管理装置3 0 δでは、リスト正当性確認機能3 7 δが図4 3で説明した処理手順に従って転送されてきたチームデータリスト

の正当性の検証を行い（ステップS 6 3 δ）、その正当性が検証できた場合に転送されてきたチームデータリストをAUD・AUL変更機能3 8 δに引き渡す。AUD・AUL変更機能3 8 δは、メンバBからの指示内容に従って、引き渡されたチームデータリストのうちオーソリティデータ1 0 3 d δについてチームマスタをメンバXからメンバZに変更して、この変更されたオーソリティデータと引き渡されたオーソリティリストとをデジタル署名機能3 9 δに送る。デジタル署名機能3 9 δは送られたチームデータリストに対してそれぞれ前述した秘密鍵ファイル等からメンバBに関する秘密鍵を取得してデジタル署名を施し、それによってオーソリティデータ1 0 3 d b δ及びオーソリティリスト1 0 3 u b δを作成（ステップS 6 4 δ）したのち、これらチームデータリストをチームデータリスト保管装置3 1 δに転送して保存要求を行う（ステップS 6 5 δ）。

チームデータリスト保管装置3 1 δでは、権限確認機能3 5 δが転送されてきたチームデータリストを基に図4 4に示した手順に従った権限確認を行って、その正当性が確認された場合に、転送されてきたチームデータリストを記憶装置3 2 δに保存する。ここで、サブチーム作成時（図4 1のステップS 2 1 δ）と相違する点は、チームマスタ変更処理においてはオーソリティリスト1 0 3 u b δのデジタル署名者であるメンバBとオーソリティデータ1 0 3 d b δで指名されているチームマスタたるメンバZが異なっていることである（ステップS 5 4 δの判断結果が“NO”となるケース）。そこでこの場合、権限確認機能3 5 δはオーソリティリスト1 0 3 u b δのデジタル署名者が親チームに登録された管理者たるチームマスタA、サブオーソリティB、サブオーソリティCの何れかに一致していれば、正当な権限を持つ者によるデジタル署名であると判断する。そして以上のようにして、サーバSV δ側にはチーム1 0 3 δに関わるチーム

データリストとして作成時間の異なる2組のオーソリティリスト及びオーソリティデータ、即ちチームマスタ変更前後の各チームデータリストが保存される。その後、チームデータリスト保管装置31δは、チーム103δの新たなチームマスタであるメンバZのデジタル署名をオーソリティリスト103ubδに付与するために、オーソリティデータ103dbδ及びオーソリティリスト103ubδをチームデータリスト管理装置30δに転送する（ステップS66δ）。

チームデータリスト管理装置30δでは、リスト正当性確認機能37δが図43の処理手順に従って、転送されてくるチームデータリストの正当性を検証したのち、これをAUD・AUL変更機能38δを介してデジタル署名機能39δに渡す。デジタル署名機能39δは、前述した秘密鍵ファイル等からメンバZに関する秘密鍵を取得し、これを基にオーソリティリスト103ubδに対してメンバZのデジタル署名を行ってオーソリティリスト103ucδを作成する（ステップS67δ）。次いで、デジタル署名機能39δは作成されたオーソリティリスト103ucδをオーソリティデータ103dbδとともにチームデータリスト保管装置31δに転送する（ステップS68δ）。チームデータリスト保管装置31δでは、権限確認機能35δが転送されてきたチームデータリストを基に図44の処理手順に従って権限確認を行い、その正当性が確認された場合に転送されてきたチームデータリストを記憶装置32δに保存して、チーム103δに関わるチームデータリストの更新処理を行う。以上によって、チームマスタが正常な手順を踏んで変更されたことになる。

#### 〈サブオーソリティの変更〉

次に、サブオーソリティを変更するための処理手順について図46を参

照して説明する。ここでは、ルートであるチーム101δのチームマスタAδが、このチーム101δでサブオーソリティとして登録されているメンバBδの作成権限を剥奪する場合を例に挙げて説明する。これは、部長代理が異動になるなどして、人事部長がこの部長代理を人事部から除外する場合などに相当する。なお、同図では図45に示したチームマスタ変更によってサブオーソリティBδが作成者となっているチーム103δを前提としている。また、同図では、サブオーソリティBの作成権限が削除されるのに伴ってチーム103δを削除してしまう場合と、チーム103δを継続させる場合の2つのケースを併せて図示してある。したがって、メンバAがチームデータリスト管理装置30δに対して要求を指示する場合にはチーム103δを存続させるかのか否かも併せて指示するようにしている。

まず、チームデータリスト管理装置30δはチーム101δに登録されているサブオーソリティBδに対する変更要求（削除要求）をチームデータリスト保管装置31δに対して送出する（ステップS71δ）。これにより、チームデータリスト保管装置31δはチーム101δの配下にあるサブチームのオーソリティデータを参照して、それらサブチームの中からサブチームBが作成者となっているチーム103δを検索したのち、チーム101δとチーム103δに関するチームデータリストをチームデータリスト管理装置30δ側に転送する（ステップS72δ）。チームデータリスト管理装置30δでは、リスト正当性確認機能37δが図43で説明した処理手順に従って、転送されてきたチームデータリストの正当性の検証を行い、その正当性が検証できた場合に転送されてきたチームデータリストをAUD・AUL変更機能38δに引き渡す。

AUD・AUL変更機能38δはメンバAからの指示内容に基づいて、引き渡されたチームデータリストのうち、オーソリティリスト101uδに記述されているサブオーソリティの中からメンバBを削除したオーソリティリスト101ubδを作成する(ステップS73δ)。これに加えて、AUD・AUL変更機能38δはオーソリティデータ103dbδに付与されているメンバBのデジタル署名を削除してオーソリティデータ103dcδを作成する(ステップS74δ)。その後、AUD・AUL変更機能38δはオーソリティデータ103dcδとオーソリティリスト103ucδをデジタル署名機能39δに送出する。

デジタル署名機能39δはメンバAからの指示内容に従って以下の2通りの処理の何れかを行う。第1に、チーム103δを継続させる要求が来ているのであれば、デジタル署名機能39δはチーム103δの存在をメンバAが承認したものと見なし、前述した秘密鍵ファイル等からメンバAに関する秘密鍵を取得し、これを基にオーソリティデータ103dcδにメンバAのデジタル署名を添付してオーソリティデータ103ddδを作成する(ステップS75δ)。次いで、デジタル署名機能39δはオーソリティデータ101dδ、103ddδ及びオーソリティリスト101ubδ、103ucδをチームデータリスト保管装置31δに転送してこれらチームデータリストの保存要求を行う(ステップS76δ)。チームデータリスト保管装置31δでは、権限確認機能35δが転送されてきたチームデータリストを基に図44に示した手順に従った権限確認を行って、その正当性が確認された場合に、転送されたチームデータリストで記憶装置32δの内容を更新する(ステップS77δ)。

第2に、チーム103δを消去する旨の要求が来ているのであれば、デ

デジタル署名機能 3 9 δ はチーム 1 0 1 δ に関するチームデータリスト、すなわちオーソリティデータ 1 0 1 d δ 及びオーソリティリスト 1 0 1 u b δ をチームデータリスト保管装置 3 1 δ へ転送するとともに、チーム 1 0 3 δ を無効にする旨の命令をチームデータリスト保管装置 3 1 δ に送出する（ステップ S 7 8 δ）。チームデータリスト保管装置 3 1 δ では、権限確認機能 3 5 δ が記憶装置 3 2 δ に保存されているオーソリティリスト 1 0 1 u δ と送られてきたオーソリティリスト 1 0 1 u b δ を照合することでサブオーソリティ B の削除を認識することができる。これに加えて、権限確認機能 3 5 δ はオーソリティデータ 1 0 1 d δ 及びオーソリティリスト 1 0 1 u b δ の内容から、チームマスタがメンバ A であって且つこれらチームデータリストが何れもこのメンバ A によってデジタル署名されていることが分かる。こうしたことから、権限確認機能 3 5 δ はチームマスタ A が正当な権限でサブオーソリティ B δ を削除したものと判断して、オーソリティデータ 1 0 1 d δ 及びオーソリティリスト 1 0 1 u b δ の内容で記憶装置 3 2 δ 中のチーム 1 0 1 δ のチームデータリストを更新する。次いで、権限確認機能 3 5 δ は記憶装置 3 2 δ 上からチーム 1 0 3 δ に関わるオーソリティデータ及びオーソリティリストを削除する（以上、ステップ S 7 9 δ）。以上によって、サブオーソリティ B の作成権限がサーバ S V δ 上のチームデータリストから削除されたことになる。

#### 〈サブチームの削除〉

次に、サブチームを削除するための処理手順について図 4 7 を参照して説明する。ここでは、ルートであるチーム 1 0 1 δ にサブオーソリティとして登録されているメンバ C が、前述した図 4 1 の処理手順で作成したチーム 1 0 3 δ を削除する場合を例に挙げて説明する。これは、人事部の下にある人事一課が廃止されたために、人事部長代理が課の廃止に関わる業

務を行う場合などに相当する。ここで、メンバCは、サブチームであるチーム103δの親に相当するチーム101のサブオーソリティの権限でもってチーム103δを削除するため、自分が間違いなくメンバC本人であることをチームデータリスト保管装置31δに対して証明してやる必要がある。そのため、チームデータリスト管理装置30δは後述するようにチームデータリスト保管装置31δに対してメンバCのデジタル署名を通知するようにしている。

さて、まずメンバCがチームデータリスト管理装置30δに対してチーム103δの削除指示を行うと、チームデータリスト管理装置30δはデジタル署名機能39δによってメンバCのデジタル署名を作成したのち、チーム103δをメンバCの権限で削除する旨の命令とメンバCのデジタル署名を組にしてチームデータリスト保管装置31δへ転送する（ステップS81δ）。なお、デジタル署名を添付する以外の方法として、削除命令の転送時に証明する「シェイクハンド」あるいは「チャレンジレスポンス」と呼ばれる方法（詳細は後述）を採用することも考えられるが、ここではデジタル署名を用いた方法に沿って説明を行うものとして、最後にシェイクハンドについて説明することとする。

チームデータリスト保管装置31δがチームデータリスト管理装置30δからチーム103δの削除命令を受け取ると、権限確認機能35δはチーム101δ及びチーム103δに関するチームデータリストを参照して、チーム101δに登録されているサブオーソリティCがチーム103δの作成者であることを知る。また、権限確認機能35δはオーソリティデータ103dδに記述されたメンバCのデジタル署名と削除命令に添付されているメンバCのデジタル署名を照合して、これらが一致していることこ

とを確認することにより、削除を指示した者が間違いなくメンバC本人であることについて確証を持てる。こうして、権限確認機能35δは正当な権限で発行された削除命令であるものと判断して、記憶装置32δ上からチーム103δに関するオーソリティデータ103dδ及びオーソリティリスト103uδを削除する（以上、ステップS82δ）。以上によって、サブオーソリティCによるチーム103δの削除処理が完了したことになる。

ところで、メンバAはチーム101δのチームマスタであることから、サブオーソリティCの代わりにサブチームたるチーム103δを削除する正当な権限を有している。この場合に、メンバAがチームデータリスト管理装置30δに対してチーム103δの削除指示を行うと、チームデータリスト管理装置30δはデジタル署名機能39δによってメンバAのデジタル署名を作成して、チーム103δをチームマスタAの権限で削除する旨の命令とメンバAのデジタル署名をチームデータリスト保管装置31δへ転送する（ステップS83δ）。チームデータリスト保管装置31δにおいて、権限確認機能35δはチーム101δ及びチーム103δに関するチームデータリストを参照することで、チーム101δに登録されているサブオーソリティCがチーム103δの作成者であり、且つ、このサブオーソリティCは親チーム101δのチームマスタAによってサブオーソリティとして指名されたものであることが分かる。また、権限確認機能35δはオーソリティデータ101dδに記載されているメンバAのデジタル署名と削除命令に添付されているメンバAのデジタル署名を照合することで、削除を指示した者が間違いなくメンバA本人であることを確認する。こうして、権限確認機能35δは正当な権限で発行された削除命令であるものと判断して、記憶装置32δ上からチーム103δに関するオーソリ



ティデータ 103 d δ 及びオーソリティリスト 103 u δ を削除する（以上、ステップ S 84 δ）。

以上によって、チームマスタ A によるチーム 103 δ の削除処理が完了したことになる。なお、上述したメンバ以外にも、例えばチーム 101 δ にサブオーソリティとして登録されているメンバ B がサブチームであるチーム 103 δ を削除することも可能である。

最後に、図 48 を参照しつつ、上述したシェイクハンドないしチャレンジレスポンスの処理手順の詳細を説明する。まず、クライアント CL δ はサーバ SV δ にアクセスする際にユーザ（図 47 の場合で言えばメンバ C またはメンバ A）のユーザ名およびユーザ公開鍵をサーバ SV δ に送付する（ステップ S 101 δ）。サーバ SV δ は乱数を発生させて内部に記憶するとともにこの乱数をユーザ公開鍵で暗号化（ステップ S 102 δ）し、暗号化されたデータを「チャレンジデータ」としてクライアント CL δ に送信する（ステップ S 103 δ）。クライアント CL δ はサーバ SV δ から送られたチャレンジデータをユーザ公開鍵に対応した秘密鍵で復号化（ステップ S 104 δ）し、得られた復号化データを「チャレンジレスポンス」としてサーバ SV δ に返送する（ステップ S 105 δ）。サーバ SV δ はクライアント CL δ から送られたチャレンジレスポンスとステップ S 102 δ で発生させた乱数とを比較して通信相手を確認する。すなわち、両者が一致すればステップ S 101 δ で送付されたユーザ公開鍵に対応する秘密鍵を知っている者が通信相手であることを確認（認証成功）することができる。これに対し、両者が不一致であれば通信相手が正当な権限を持った者でない可能性のある（認証失敗）ことがわかる（以上、ステップ S 106 δ）。この後、サーバ SV δ はステップ S 106 δ で得られた確

認結果（認証成功または認証失敗）をクライアントCL $\delta$ に通知する（ステップS107 $\delta$ ）。以上のようにすることで、デジタル署名を添付した場合と同じく、メンバCやメンバAが本人であることをサーバSV $\delta$ 側で確かめることができる。

なお、クライアントCL $\delta$ からサーバSV $\delta$ へユーザ公開鍵を送る代わりに「ユーザ公開鍵番号」を送るようにしても良い。ここで言うユーザ公開鍵番号はユーザ本人を識別・認証するための情報であって、各ユーザ公開鍵に予め付与されているシリアル番号のことである。さらに詳しく説明すると、ユーザ公開鍵番号はユーザ公開鍵を一意に識別するための各ユーザ公開鍵に対応した情報であって、例えば、上述した認証局から発行された証明書に含まれている当該証明書のシリアル番号である。また、ユーザ本人を識別・認証するための情報としては、いま述べたユーザ公開鍵番号以外にも、実際に鍵作成者本人を識別するIDや名前などの様々な情報を利用することができる。

#### 〔第4－2実施形態〕

図49は本実施形態によるチームの階層化について示したものであって、チーム内のメンバの利用できるアプリケーションがチーム毎に異なる形態を実現したものである。同図では、図40に示したチームのうちチーム101 $\delta$ ～103 $\delta$ に対応するものだけを示してある。オーソリティリスト及びオーソリティデータに関しては図40に示したものと同じであるが、このほか、各チームにはメンバリストの代わりにメンバリストの内容を包含するアプリケーションリスト101a $\delta$ 、102a $\delta$ 、103a $\delta$ が設けられている。すなわち、これらアプリケーションリストには、各チームに属するメンバの利用可能なシステムのほか、そのチームに属するメンバ

の一覧が記載されている。アプリケーションについては例えばチーム 1 0 1 δ のアプリケーションリスト 1 0 1 a δ には人事管理システム、経理システム、スケジュール、ファイル共有システムが登録されている。また、メンバー一覧については図 4 0 のメンバリストに記載されているものと同じである。

この第 4 - 2 実施形態では、第 4 - 1 実施形態と同様にチームの生成に関しては親チームの干渉を受けるものの、アプリケーションリストは各チームのチームマスタがそれぞれデジタル署名するので、チーム内の管理は親チームからの干渉を受けずに行うことができる。つまり、チーム内で利用可能なアプリケーションをどのメンバで共同利用するかといったことは、チームマスタが親チームの管理者から独立して行うことができる。例えば、チーム 1 0 1 δ のサブチームであるチーム 1 0 2 δ では、アプリケーションリスト 1 0 2 a δ のデジタル署名はチーム 1 0 2 δ のチームマスタであるメンバ Y δ がデジタル署名しており、チーム 1 0 1 δ の管理者であるチームマスタ A δ やサブオーソリティ B δ、C δ の干渉を受けなくて済む。

#### 〔第 4 - 3 実施形態〕

本実施形態では、サブチームを管理するという観点から見たメンバ、サブオーソリティ、チームマスタという上述の権限分担に加えて、情報を共有してゆくためのチーム内での管理権限分担として各チームに属する者をメンバ、サブマスタ

、チームマスタの 3 種類に分類している。このうち、サブマスタはチームマスタによって指名されたチーム内の管理者であって、チームマスタやサブマスタを変更することは許されていないが、一般のメンバについて追加、削除、変更を行うことのできる者である。一方、チームマスタはサブマス

タ又はメンバの変更を行えるほか、自身のチームマスタでさえ変更することのできる者である。他方、サブマスタ及びチームマスタ以外の一般のメンバはメンバに提供される情報や機能を共有する者であって、チームデータリストの内容に変更を加える等の権限はいっさい与えられていない。なお、サブマスタやチームマスタも特別な権限が与えられてはいるが、チーム内のメンバであることに変わりはなく、その意味でサブマスタ又はチームマスタをメンバと呼ぶことがある。

図50は本実施形態におけるチームの階層化について示したものである。同図では、図40に示した第4-1実施形態の各チームに対してさらにチームマスタリストを加えてある。こうすることで、チーム毎に情報共有を管理するとともに、各チーム内の情報共有のメンバの管理を複数の管理者が行えるようにしている。図50において、チームマスタリスト101t $\delta$ ~104t $\delta$ は各チームに登録されているチームマスタ及びサブマスタの一覧とチームマスタのデジタル署名が記載されている。もともと、これ以外にもチームマスタリストには、チームマスタ又はサブマスタの識別情報、公開鍵、公開鍵ID、チームID、チームマスタリストの作成時間を示すタイムスタンプなどが含まれている。このほか、チームマスタリスト34 $\delta$ には、チームに関する情報としてチームのメンバ数、チームの作成された時間、チーム内の各メンバが利用することのできる各種機能などの情報（例えば、上述したアプリケーションリスト）も含まれており、これらを用いることで各チームに関する情報リソースの管理を同時に行うことができる。

チームマスタリストのデジタル署名は、各チームのチームマスタがチーム作成時にデジタル署名し、以後はずっとチームマスタのデジタル署名に

なっている。これに対し、メンバリストについては各チーム内のチームマスタの他に、サブマスタがこれを管理する権限を付与されているため、チームマスタ以外にサブマスタのデジタル署名が為されている場合もある。例えば、メンバリスト 1 0 1 m a δ に関してはチーム 1 0 1 δ のサブマスタとして登録されているメンバ B δ のデジタル署名がなされている。一方、チーム 1 0 2 δ のように、チームマスタリスト 1 0 2 t δ にサブマスタが登録されていない場合にはメンバリスト 1 0 2 m a δ はチームマスタであるメンバ B δ がデジタル署名することになる。

この図 5 0 ではサブチームの管理権限、メンバの管理権限をそれぞれオーソリティリスト／オーソリティデータ、チームマスタリストに分割しているため、各チーム内でサブオーソリティとサブマスタに異なる者を割り当てることができる。例えば、チーム 1 0 3 δ ではメンバ W 及びメンバ V がサブオーソリティであり、メンバ Y 及びメンバ Z がサブマスタであるため、サブチームの管理とメンバ管理を異なる者が担当して負荷分散を図ることもできる。もともと、実際にはサブオーソリティとサブマスタを同じメンバにしてしまっても良い。その場合はオーソリティリストとメンバリストを統合して一つのリストにしてしまうことが可能となる。

#### 〔第 4 - 4 実施形態〕

上述した各実施形態では、チームデータリストを使用する都度、チームマスタが間違いなく自分のチームマスタであるかどうかをユーザがクライアント C L δ 側で確認する必要がある。例えば、チームデータリスト管理装置 3 0 δ を構成するコンピュータのディスプレイ上に、“このリストは以下のメンバが管理者となって正常に管理されています。名前：メンバ A。組織：三菱マテリアル株式会社。作業を続行する場合は O K ボタンをマウ

スでクリックして下さい”などといったメッセージが表示される。このように、ユーザは当該メッセージを目視で確認する必要が生じてくるため、ユーザに対して煩わしい印象を与える可能性がないとは言えない。こうした点を改善するには以下の機能をリスト正当性確認機能 37δ と連携する新たな機能として追加し、あるいは、リスト正当性確認機能 37δ の一機能として組み込むようにすることで解決される。

すなわち、ルートチーム 101δ におけるチームマスタの公開鍵をチーム毎に予めクライアント CLδ 側の例えば公開鍵データベース 41δ (図 37 参照) に登録しておき、公開鍵管理機能 40δ が公開鍵データベース 41δ からチーム 101δ のチームマスタに関する公開鍵を取得してこれをリスト正当性確認機能 37δ に通知する。もしくは、公開鍵データベース 41δ には公開鍵に関する情報として公開鍵を識別するためのシリアル番号等を登録しておき、公開鍵管理機能 40δ がこのシリアル番号を公開鍵データベース 41δ から取得したのち、これをもとにチームデータリスト管理装置 30δ の外部 (例えばインターネット上) に登録されている公開鍵を別途取得してリスト正当性確認機能 37δ に渡すように構成しても良い。

一方、リスト正当性確認機能 37δ は、コンピュータのディスプレイ上に上述したようなメッセージを出す代わりに、公開鍵管理機能 40δ から通知されるチーム 101δ のチームマスタの公開鍵に基づいて、チームデータリスト保管装置 31δ から転送されてくるオーソリティデータ 101dδ に含まれているチームマスタのデジタル署名を確認するようにして、当該デジタル署名が登録されているチームマスタのものかどうかを判断する。こうすることで、ユーザがディスプレイ上の表示をもとに目視で確認

することなく、ルートチーム 101δ のチームマスタの正当性を検証できるようにする。

なお、チームマスタを確認するための情報としては公開鍵以外にも様々な情報を利用できるのはもちろんである。

以上の通り、チームを階層化するためのチームデータリストを管理するチームデータリスト管理プログラムを記録した記録媒体において、チームデータリスト管理プログラムは、(1) 所定の要求先に前記チームデータリストの操作要求を行う処理と、(2) 前記操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理者のデジタル署名が含まれたオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者のデジタル署名が含まれたオーソリティリストを有するチームデータリストを前記要求先から取得する処理と、(3) 前記識別子を用いて取得された各チームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストのデジタル署名が改竄されていないこと及び前記管理者情報を用いて権限を持つ者によるデジタル署名であることを確認したのち、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認処理と、(4) 該正当性確認処理によって正当性が確認された前記チームデータリストに対して前記操作要求に応じた変更を加える変更処理と、(5) 前記操作要求を行った指示者のデジタル署名を作成して、前記変更処理によって変更されたチームデータリストに該デジタル署名を添付して前記要求先に送付する処理とをコンピュータに実行させる。

また、上述のチームデータリスト管理プログラムにおいて、前記正当性

確認処理は、前記チームマスタにより自チーム内のメンバから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報を前記管理者情報として用いるものであっても良い。

また、上述のチームデータリスト管理プログラムは、前記ルートチームのチームマスタの本人識別を行うための識別情報を所定の場所から取得して予め登録しておく処理と、前記要求先から前記ルートチームのオーソリティデータが送られてくる度に、予め登録されている前記識別情報を用いて、該オーソリティデータのデジタル署名が前記チームマスタのデジタル署名であることを確認する処理とをさらにコンピュータに実行させるものであっても良い。

一方、チームを階層化するためのチームデータリストを保管するチームデータリスト保管プログラムを記録した記録媒体において、チームデータリスト保管プログラムは、(1) 自チームの親チームを表す識別子及び前記親チームの管理者のデジタル署名が含まれたオーソリティデータをチーム毎に予め記憶しておく処理と、(2) 自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者のデジタル署名が含まれたオーソリティリストをチーム毎に予め記憶しておく処理と、(3) 所定の要求元から前記オーソリティデータ及び前記オーソリティリストが少なくとも含まれたチームデータリストに対する操作要求があったときに、該操作要求の指示者が要求権限を持つことを前記管理者情報を用いて確認するとともに、該操作要求が参照要求或いは削除要求である場合は、要求されたチームデータリストを前記要求元へ返送し或



いは削除し、該操作要求が更新要求である場合は、前記要求元から送られるチームデータリストのデジタル署名が権限を持つ者によるデジタル署名であることを前記管理者情報を用いて確認したのち、前記送られたチームデータリストで記憶されている前記オーソリティデータ及び記憶されている前記オーソリティリストを更新する権限確認処理とをコンピュータに実行させる。

また、上述のチームデータリスト保管プログラムにおいて、前記権限確認処理は、前記チームマスタにより自チーム内のメンバから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報を前記管理者情報として用いるものであって良い。

以上説明したように、第4-1～4-4の実施形態の発明には以下の効果がある。

本発明では、オーソリティリストとオーソリティデータの含まれたチームデータリストを用いることで各チームの下にサブチームを作成することができ、階層化されたチームを構築することができる。また、ユーザはルートチームのチームマスタのデジタル署名を確認するだけで、操作対象のチームからルートチームに至る各チームについてチームデータリストの正当性を確認することができる。さらに、親チームの管理者の指示によって誰もがサブチーム内の管理を行うチームマスタになることができる。

また、本発明では、チームデータリストを親チームの管理下にあるオーソリティデータと自チームの管理に関わるオーソリティリストに分割しており、各チームのチームマスタが親チームの干渉を受けることなく情報共有メンバの管理といった自チーム内の管理を行うことができ、一方で、親

チームの管理者はサブチーム内部の管理に関与する必要がなくなる。

また、本発明では、チームデータリストに対して正当な権限を持つ者によるデジタル署名を含ませているため、改竄等の不正な行為を検出することが可能となる。また、本発明では、チームデータリストの操作要求がなされた場合に、これら要求の指示者が権限を持つ者かどうかの権限確認を実施しているので、サーバの管理者、チーム内の一般のメンバ、クラッカ等の権限を持たない者による不正な行為を未然に防止することができる。

また、本発明では、特に選定されたチームマスタと一人以上のサブオーソリティに対してサブチームの管理権限を与えており、チームマスタ自身がサブオーソリティを選任できるほか、複数の管理者がサブチームを管理できるため管理負担が分散される。

また、本発明では、公開鍵などのルートチームのチームマスタ本人を識別・認証するための識別情報を予め登録しておき、この識別情報をもとに、ルートチームのチームマスタを確認しているため、チームデータリストを操作する度にユーザ自身が目視で確認するなどの煩わしい作業が必要なくなり、ルートチームのチームマスタを自動的に承認することが可能となる。

第5-1a～5-4a、第5-1b～5-3b、第5-1c～5-5c、第5-1d～5-6dの実施形態の発明は、コンピュータネットワークを利用した同報通信の分野にあって、同報通信に利用される情報中継装置の管理者による不正を防止できる同報通信システムに関する。

第5-1a～5-4a、第5-1b～5-3b、第5-1c～5-5c、第5-1d～5-6dの実施形態の発明に関し、従来以下説明する技術が知られている。

近年、インターネット等のオープンなネットワークの普及によって、企

業等の組織が持つLAN内だけではなく、インターネットに接続されたさまざまなメンバーと同報通信を行うことができるようになっている。同報通信とは、通信網上の多数の端末に同じ情報を一度に送信することを目的とした通信をいい、例えば電子メールシステムの場合には、メーリングリストを利用することによって同報通信を実現している。また、他の同報通信の例として、リアルタイムチャットなどもあげられる。

現在実現されている同報通信システムの一般的な例では、送信側端末は、同報通信を行うメッセージを受信者（被配信者）の集合（配信先リスト）を管理する情報中継装置に転送する。そして情報中継装置が配信するメッセージを受信者数分複製し、同報通信の各受信者に対して転送することにより同報通信を実現している。例えば、図64に示す電子メールシステムでは、受信者の集合を示すメーリングリスト（List 01）を管理するメーリングリスト管理ホスト（Server A）に対してメッセージを送り、このメーリングリスト管理ホストがメーリングリストに挙げられている各受信者（User A、User B、User C）に対してメッセージをコピーして送ることにより同報通信を実現している。

しかし、前述のようなオープンなネットワークアーキテクチャー上に構築された同報通信システムでは、各受信者に配信されるメッセージの覗き見や第三者への機密情報の漏洩等が常に問題となっていた。このような問題点を省みて、今日まで、EDI（Electronic Data Interchange）やEC（Electronic commerce）のようなネットワーク上における機密情報転送のニーズが高まり、同報通信システムにおいても、暗号技術を利用してセキュリティを高めた同報通信システムが研究・開発されている。

暗号技術を利用してセキュリティを高めた同報通信システムとして、特開平 6-152592 に開示されている同報通信システムがある。この発明では、暗号化に利用するデータ鍵と受信者を特定する宛先情報とシステムで共通のマスタ鍵とに基づいて暗号化鍵を生成し、この宛先情報と暗号化鍵を通信者間で送受信することにより、任意の一人または複数の通信相手とデータ鍵をを共有できる暗号通信方式を開示している。

しかし、このシステムを利用するにあたっては、セキュリティを確保するために、グループに属するメンバーを設定しておき、このメンバーに対しては、グループで暗号通信を行うために、ICカード等の記憶媒体を配布しておく必要がある。しかし、現在利用されている同報通信（例えば、メーリングリスト）においては、グループに属するメンバーは脱退、加入等により動的に変化し、随時、配信先が変わるため、暗号同報通信においても、このような脱退、加入等に対応できることが望ましい。

次に、図 65 に示す特開平 7-245605 に開示されている同報通信システムでは、メンバーの加入・脱退にも柔軟に対応できる同報通信システムを開示されている。この同報通信システムにおける暗号化情報中継装置（Server A）は、通信回線で接続された複数の加入者間で情報の送受信を行うシステムにおいて、発信加入者から送信され受信した暗号化情報の復号化(②)、または、受信加入者に送信する情報の暗号化(③)を行なう暗号計算部と、暗号化情報を復号化するための共通秘密鍵と、各加入者（User A、User B、User C）に対応した暗号化を行うための各加入者毎の個別公開鍵とを格納した鍵格納部とを有する暗号化情報中継装置をもつ。

しかし、この情報中継装置の管理者、もしくは、この管理者によって権限を委譲された者は、たとえ同報通信の加入者の中に含まれていない場合でも、暗号通信の通信内容を覗き見することができる。よって、悪意ある情報中継装置の管理者が存在する場合には、暗号通信で転送される機密情報が漏洩する危険性がある。例えば、企業間で行う同報通信での機密情報として企業の合併情報などが挙げられるが、これは、合併の影響を受ける情報中継装置の管理者に漏洩してはいけない情報である。

また、この情報中継装置は、必ず、暗号化情報の復号化处理、暗号化处理を行うことになる。しかし、暗号化处理・復号化处理は複雑で、大きな処理能力を必要とする。よって、同時に多数の暗号化情報が情報中継装置に到着した場合には、同報通信の遅延や、情報中継装置の処理能力を超えたために、動作不能に陥る危険性がある。

企業や組織、個人等が漏洩すると大きな損害を被るであろう機密情報を、限定された複数のメンバー間だけで同報通信を行うためには、以下のような課題を解決した同報通信システムを実現する必要がある。

(1) 情報中継装置の管理者といえども、同報暗号通信の通信内容は、覗き見できない仕組みを実現し、本当に情報を共有する必要のあるメンバーにだけ同報通信内容が見られるようにする。

(2) 同報通信を行う受信者の脱退や、加入に対して迅速に対応でき、同報通信メンバーの動的な変更があっても、誤って同報通信してはいけないメンバーに情報を転送してしまうことを防止できるようにする。

(3) サーバ管理者が同報通信の配信メンバーを管理するのではなく、同報通信を行うメンバーの中で配信メンバーを管理し、さらにメンバーの管理者に集中する管理負担をできるだけ軽減する。

(4) 機密情報を転送するため、多数の受信者それぞれが、確実に受信

できる仕組みを確立する。

第5-1a～5-4a, 第5-1b～5-3b, 第5-1c～5-5c, 第5-1d～5-6dの実施形態の発明は、上記の点に鑑みてなされたもので、上記課題を解決する同報通信システムを構成するメンバーリスト管理装置、暗号情報作成装置、情報中継装置、暗号情報復号化装置、および、こららをコンピュータに実現させるプログラムを記録した記録媒体を提供するものである。

まず、第5-1a～5-4a, 第5-1b～5-3b, 第5-1c～5-5c, 第5-1d～5-6dの実施形態の発明の同報通信システムを構成するメンバーリスト管理装置、暗号情報作成装置、情報中継装置、暗号情報復号化装置の各実施の形態の説明にあたり、本発明の基本的技術思想および実施の形態の説明に用いる用語を説明する。図52に本発明の同報通信システムの概要を示している。なお、本発明の同報通信システムを構成する各装置の実施の形態は後ほど詳細に説明する。

上述したように、従来の同報通信では、情報中継装置（サーバ）に保存された被配信メンバー（受信者）の設定は、主にサーバ管理者、もしくは、サーバ管理者によって権限を委譲された者によって管理されていた。しかし、機密情報を同報通信する場合には、サーバ管理者が管理すべきでない同報通信を行う可能性がある。

そこで本発明では、サーバ管理者ではなく、同報通信メンバー内のメンバーを管理する管理者（以降、チームマスターと称す）による被配信メンバーのリスト（以降、メンバーリストと称す）の管理を実現し、このメン

バーリストが他者に改竄されない仕組みを提供する。そして、メンバーリストが安全かつ確実にメンバーリストに含まれるメンバーで共有され、メンバーが発信する同報通信の情報内容は暗号化され、情報が漏洩することなく、同報通信メンバーが安全かつ確実に機密情報を受信できるようにするものである。

まず、機密情報を安全かつ確実に同報通信をするには、通信相手となるメンバー本人を識別・認証する仕組みが必要となる。本発明では、本人を識別するための手法として、公開鍵暗号方式（例えば、R S A（Rivest-Shamir-Adleman）方式や楕円暗号方式）における秘密鍵が、本人のみによって所有される仕組みを利用する。そのため、本発明のメンバーリストには、少なくとも、秘密鍵に対応する公開鍵が含まれる。また、メンバーリストが安全に管理されるようにするため、他者によって改竄されない仕組みを実現するため、チームマスターによるデジタル署名を添付する。

メンバーリストは、一般的には、チームマスターによって管理されるが、例えば、同報通信のメンバーの数が多く、一人の管理者で管理できない場合には、メンバーリストを複数のリストにわけ、チームマスターリストに含まれる複数の管理者（チームマスターと、チームマスターから権限を与えられたサブマスター）によって、管理される場合がある。図53に示すように、一般的なメンバーリストは、チーム名、チームマスターであるメンバーXの名前もしくは識別子と、チームのメンバーであるメンバーY、…、メンバーBの名前もしくは識別子と、このメンバーリストに対するチームマスターXのデジタル署名からなる。また図54に、前述したようにメンバーリストが複数のリストからなる場合、特にメンバーリストをチーム101εの管理者を登録したチームマスターリストと、チーム101ε

の同報通信メンバーを登録したメンバーリストに分割した場合の例を示している。この例のメンバーリストのデジタル署名は、チームマスターのXのみならず、サブマスターのY、Zのデジタル署名であってもメンバーリストの正当性を確認できる。

この場合には、まず、メンバーリストのデジタル署名より、メンバーリストが改竄されていないかを検証し、デジタル署名者（この例では、メンバーX）を特定する。次に、チームマスターリストのデジタル署名より、チームマスターリストが改竄されていないかを検証し、さらにチームマスターのデジタル署名者が間違いなくこのチームのチームマスターかどうかを確認する。最後にこのメンバーリストのデジタル署名者が、チームマスターリストにチームの管理者として登録されているかを検証する。図54の例では、メンバーXは、チームマスターとして登録されているので、正当なデジタル署名者であると判断できる。また、メンバーリストにメンバーYによるデジタル署名が添付されていた場合でも、メンバーYは、メンバーXより管理権限を委譲された正当なデジタル署名者（ここでは、サブマスターとする－図54中では、「サブ」と記載している）として判断できるため、正当性を検証できる。

また、メンバーリストには、一人のメンバーに対して、複数の公開鍵を登録する方式としてもよい。例えば、暗号化・復号化処理に利用する公開鍵と秘密鍵のペアと、デジタル署名作成・検証処理に利用する公開鍵と秘密鍵のペアを、それぞれ異なる鍵ペアを利用する場合には、各メンバーに対して2つの公開鍵が登録されていることになる。

また、メンバーリストには公開鍵を登録するが、この公開鍵として認証



局より発行されたデジタル証明書（例えば、X. 509フォーマットに従ったデジタル証明書であり、以降、証明書と称す）を利用することができる。また、メンバーリストに、公開鍵本体を一意に識別するための情報を登録する方式を利用してもよい。この場合は、公開鍵本体は、各メンバーがすでに保有している場合には、公開鍵を識別する情報（例えば、信頼できる認証局より発行された証明書に含まれる公開鍵を利用している場合には、その証明書に与えられたシリアルN oや認証局名、証明書をハッシュ関数で圧縮したメッセージダイジェスト）をメンバーリストに含めておけば、各メンバーは、メンバーリストを受け取った後、暗号化に利用する実際の公開鍵本体を選択もしくは、取得することができる。例えば、メンバーリストに認証局名とシリアルN oが含まれていた場合には、まず、端末に接続された記憶媒体に保存された複数の証明書から、この認証局名とシリアルN oをもつ証明書を検索し、記憶媒体に存在しなかった場合には、この認証局名の認証局に問い合わせこのシリアルN oの証明書を取得することもできる。

以下に、第5-1 a～5-4 a，第5-1 b～5-3 b，第5-1 c～5-5 c，第5-1 d～5-6 dの実施形態の発明の同報通信システムを構成するメンバーリスト管理装置、暗号情報作成装置、情報中継装置、暗号情報復号化装置の各実施の形態を図面を参照し順に説明する。

図55は、本発明のメンバーリスト管理装置の第5-1 aから第5-4 aの実施の形態を包含し表している。

#### [第5-1 aの実施形態]

まず、メンバーリスト管理装置1εの第5-1 aの実施の形態を説明す

る。本実施の形態は、メンバーリストを管理するために、同報通信を行う  
1以上のメンバーの公開鍵を含むメンバーリストを作成するリスト作成部  
1aεと、メンバーリストに含める公開鍵を取得し保存する公開鍵管理部  
1bεとから構成される。

はじめにチームマスターが、メンバーリスト管理装置1εを利用してメンバーリストを作成するための所定の項目（メンバーの情報等）を入力する。データの入力後、図56に示すようにリスト作成部1aεは、メンバーとして登録するメンバーの公開鍵を選択する（ステップS1ε）。例えば、図53に示すメンバーリストを作成する場合、メンバーX、Y、…、Bの公開鍵が選択される。そして、ハッシュ関数（例えば、MD5やSHA-1等）を利用してメンバーリストのメッセージダイジェストを作成する（ステップS2ε）。そして、作成したメッセージダイジェストをチームマスターの秘密鍵で暗号化して（例えば、RSAやDSAを利用して）作成したデジタル署名をメンバーリストに添付（ステップS3ε；図2の例では、Xのデジタル署名を添付）する仕組みとする。この仕組みにより、後述の情報中継装置以外の端末（図示せず）をメンバーリスト管理装置1εとして利用しても、メンバーリストを改竄される心配はない。現実に改竄された場合には、メンバーリストの正当性を検証することにより改竄が発覚するため、改竄されたメンバーリストの使用を中止することが可能である。

#### [第5-2aの実施形態]

次に、メンバーリスト管理装置1εの第5-2aの実施の形態として、第5-1aの実施の形態のメンバーリスト管理装置1εに、さらにリスト取得保存部1cεを備えた構成をとる。

リスト取得保存部 1 c ε は、メンバーリスト管理装置 1 ε に接続された記憶媒体に対するメンバーリストの取得保存を行なうように動作するだけでなく、メンバーリスト管理装置 1 ε が接続されたネットワークに配置された端末（例えば、サーバ）やデータベース（図示せず）を利用して、これらの端末やデータベースにアクセスし、メンバーリストを取得または保存するように動作する。

この構成をとるのは、あるチームマスターがメンバーリストを管理している間に、チームマスターの端末に障害が発生した場合や、誤ってメンバーリストが消去される危険性があるため、チームマスターの端末でなく、ネットワーク上の安全な端末（例えば、サーバ）またはデータベースにメンバーリストを保存しておく、より安全であるからである。

また、同報通信の管理負担が一人の管理者に集中すること軽減し、操作ミス等を未然に防止するため、複数の管理者（チームマスターと複数のサブマスター）でメンバーリストを管理する形態もある。この場合、各管理者が異なるバージョンのメンバーリストを利用することが無いように、各管理者がアクセスできるネットワーク上の端末またはデータベースに、メンバーリストを保存する方がより完全性を保った同報通信を実現できる。

本発明の同報通信システムは、メンバーリストに含まれる公開鍵によって暗号化を行うことによって、同報通信メンバー外への情報の漏洩を防ぐ（例えば、サーバ管理者への情報の漏洩を防ぐ）仕組みを実現している。よって、メンバーリスト管理装置 1 ε では、メンバーリストが正当性をもって管理されているかを検証する必要がある。ここでいう正当性の検証とは、1）メンバーリストが、権利のない者に改竄されていない状態を維持している、かつ、2）メンバーリストを作成した者が同報通信を行うチー

ムの正式なチームマスターである、状態を確認することである。

1) については、例えば、メンバーリストに添付されたデジタル署名(図53の例では、メンバーXのデジタル署名)を復号化してメンバーリストのメッセージダイジェストを取得し、さらに、メンバーリスト(図53の例では、チーム101ε、メンバーX、メンバーY…メンバーBを内容としてもつリスト)をメンバーリスト作成時に用いられたものと同じハッシュ関数で圧縮して得たメッセージダイジェストを取得し、双方を比較することにより検証できる。また、2) については、例えば、メンバーリストへのデジタル署名者の名前(例えば、X. 509の証明書フォーマットに従う証明書に記載された名前)をメンバーリスト利用者が確認できるように画面に表示し、確認してもらうことにより検証できる。

リスト取得保存部1cεは、メンバーリストを識別する情報とメンバーリストを管理するチームマスターを対応づける対応テーブルを作成し保存する機能と、メンバーリストに添付されたデジタル署名の正当性を確認する際に、この対応テーブルを参照して、デジタル署名が正当なチームマスター本人のデジタル署名であるかどうかを判断させる機能をさらに備えることでメンバーリストの正当性を検証できる。

また、対応テーブルを作成するにあたっては、例えば、初めて取得するメンバーリストの場合には、メンバーリスト利用者がチームマスターを確認できるように画面に表示し、確認してもらうことにより検証する。ここで肯定指示(メンバーリストのデジタル署名者としてこのチームマスターを認める場合)が出た場合には、メンバーリストを識別する情報(図53の例では、チーム名の「チーム101ε」)とメンバーリストを管理するチームマスター(図53の例では、チームマスターである「メンバーX」)

を、テーブルに追加する追加機能をさらに備えることで、2回目以降は、自動的に正当性確認が行われるようになる。

ここで説明した、メンバーリストの正当性を検証する機能は、後述の暗号情報作成装置、暗号情報復号化装置、情報中継装置のそれぞれにおいても備えられ、メンバーリストの取得時もしくはメンバーリストを利用する際に機能する。

#### [第5-3aの実施形態]

次に、メンバーリスト管理装置1εの第5-3aの実施の形態として、第5-1aもしくは第5-2aの実施の形態のメンバーリスト管理装置1εに、リスト送信部1dεをさらに備えた構成をとる。

リスト送信部1dεは、メンバーリストに含まれるメンバーが利用する端末にメンバーリストを送信するように動作する。

この構成をとることにより、最新のメンバーリストをメンバーリストのメンバー間で迅速かつ正確に共有することができる。

また、チームマスターはさらに、後述する情報中継装置が情報を再配信する際に参照する配信先リストを変更する必要がある。この配信先リストを変更する仕組みは、情報中継装置の種類や仕組みによって異なってくる。例えば、音声チャットの同報通信システムとメールの同報通信システムでは、装置の構造やプロトコルが異なる。本実施の形態のメンバーリスト管理装置1εでは、利用するシステムによって操作方法が異なることの無いように、メンバーリストに含まれるメンバーと配信先リストに含まれるメンバーが同一になるように、メンバーリスト管理装置1εに配信先リストを変更する機能をさらに付加してもよい。この配信先リストを変更する機能として、もっとも簡単な実施形態としては、本実施の形態のリスト送信

部 1 d ε からメンバーリストを情報中継装置に転送し、情報中継装置ではこのメンバーリストを配信リストとして用いる方式があげられる。

[第 5 - 4 a の実施形態]

本発明のメンバーリスト管理装置の第 5 - 4 a の実施の形態として、第 5 - 1 a ないし第 5 - 3 a のいずれかの実施の形態のメンバーリスト管理装置 1 ε に、加入要求受付部 1 e ε をさらに備えた構成をとる。

加入要求受付部 1 e ε は、同報通信のメンバーリストへの加入要求を受け付けるために、同報通信のチームマスターが、特定同報通信の配信リストへの加入要求項目を設定する加入要求項目設定機能と、加入要求を受付ける際に加入要求者が満たすべき項目を提示するための加入要求項目提示機能と、加入要求者が転送してきた加入要求が、加入要求項目を満たし、加入を許可するか否かを判断する加入許可判断機能を備える。

また、本実施の形態の加入要求受付部 1 e ε は、加入要求が正確な要求であるかどうかを検証する際に、ネットワーク上に配置されたデータベースやサーバ等に、問い合わせて検証を行なう。例えば、加入項目にクレジットカード No が記載されていた場合には、このクレジットカード No の有効性をクレジットカード会社が運用する端末にアクセスして検証したり、証明書が含まれていた場合には、認証局が運用する証明書データベースにアクセスして検証することができる。

上述の加入要求受付部 1 e ε の機能により、同報通信への受信者の自動加入を実現することができる。現在実現されている同報通信への受信者の自動加入の一例として、例えば、メーリングリストへの加入プロセスを自動化し、ユーザが WWW ページで登録するとメーリングリストに自動的に

加入できるシステムがある。しかし、現在のメーリングリストは、情報中継装置の管理者の権限で起動されるプロセスを自動化したものであり、現在の自動化プロセスでは、情報中継装置の管理者が、配信メンバーを自由に設定できる仕組みを提供しているにすぎない。本実施の形態の加入要求受付部 1 e ε は、悪意ある情報中継装置の管理者などによる不正を防止し、より安全性の高い自動加入の仕組みを提供するためのものである。

ここで、メンバーリストに含まれる公開鍵や、秘密鍵は、間違いなく本人のものかどうか、また、使用期限などを設定していた場合に期限切れでないか、また、すでに秘密鍵が漏洩していないかを検証してから利用する方が望ましい。したがって、メンバーリスト管理装置 1 ε の各実施の形態では、ネットワーク上に配置されたデータベース（例えば、認証局やサービス企業が提供する公開鍵の有効性や信頼性をあらわす状態を登録したディレクトリデータベースなど）に、同報通信と同じまたは、異なるプロトコル（例えば、同報通信で S M T P（Simple Mail Transfer Protocol）を利用する場合には、L D A P（Lightweight Directory Access Protocol）、O C S P（Online Certificate Status Protocol）など）を利用して問い合わせを行ったり、認証局より配布される証明書廃棄リスト（C R L（Certificate Revocation List））を利用して、公開鍵やデジタル署名に利用される秘密鍵の有効性を検証する形態としてもよい。

ここで説明した、公開鍵やデジタル署名に利用される秘密鍵の有効性を検証する機能は、後述の暗号情報作成装置、情報中継装置、暗号情報復号化装置のそれぞれにおいてもこの機能を備えることにより、デジタル署名の確認やメンバーリストの管理の際に有効となる。

以上、本発明のメンバーリスト管理装置の各実施の形態を説明した。

次に、本発明の暗号情報作成装置の実施の形態を説明する。図57は、本発明の暗号情報作成装置の第5-1bから第5-3bの実施の形態を包含し表している。

[第5-1bの実施形態]

本発明の暗号情報作成装置の第5-1bの実施の形態は、ネットワークを介してメンバーリストを取得し保存するリスト取得保存部2aεと、暗号情報を作成する暗号化部2bεとから構成される。

リスト取得保存部2aεは、ネットワーク上に配置されたリソースデータベースに保存されたメンバーリストを、同報通信と同じ、または、異なるプロトコル（例えば、同報通信でSMTPを利用する場合には、HTTPなど）を利用して取得する。または、転送されてきたメンバーリストを記憶装置（図示せず）に保存し、必要なときに保存先からメンバーリストを読み込むことにより取得する。

また、暗号情報作成装置2εがすでにメンバーリストを保存している場合には、リスト取得保存部2aεは、メンバーリストが最新バージョンか確認するように動作する。例えば、メンバーリストの最新バージョンに関する情報が保存されたネットワーク上に配置されたデータベースに、同報通信と同じまたは、異なるプロトコル（例えば、同報通信でSMTPを利用する場合には、LDAP、OCSPなど）を利用して、最新のメンバーリストのバージョンを問い合わせ確認する。また、リスト取得保存部2aεは、前述のメンバーリスト管理装置1εの実施の形態で説明したメンバーリストの正当性を検証する機能を備え、メンバーリストの取得時にメンバーリストの正当性を検証する。



なお、記憶部（図示せず）は、EEPROM、ハードディスク、光磁気ディスク等の不揮発性の記憶装置により構成されている。

次に、暗号化部 2 b ε は、図 5 8 に示すようにまず同報通信文（平文）とリスト取得保存部 2 a ε により取得されたメンバーリストを取得し、同報通信文を共通鍵暗号方式（例えば、DES 等の暗号化と復号化で同じ鍵を利用する暗号方式）で暗号化し暗号文を作成する。

そして暗号文作成に用いた共通鍵を、メンバーリストに含まれる各メンバー公開鍵を用いて、公開鍵暗号方式（例えば、RSA 方式）により暗号化した暗号化鍵を作成する。このときメンバーが 3 名ならば、3 つの暗号化鍵が作成されることになる。

さらに複数の暗号化鍵のうち、被配信メンバーに対応する暗号化鍵を選択するための鍵選択情報を作成する。この鍵選択情報として、例えば、メンバー名と暗号化鍵を対応させるテーブルを用いてもよい。

また、同報通信文をハッシュ関数で圧縮し、送信者の秘密鍵で暗号化したデジタル署名を付加する。このデジタル署名により改竄防止、送信者の確認ができるようになる。

そして暗号情報として、暗号文、暗号化鍵、鍵選択情報、およびデジタル署名を出力するように動作する。

なお、同報通信システムにおいて、この暗号情報作成装置 2 ε は送信側端末で利用されるものである。

#### [第 5 - 2 b の実施形態]

次に、暗号情報作成装置 2 ε の第 5 - 2 b の実施の形態は、図 5 7 に示すように第 5 - 1 b の実施の形態に宛先検査部 2 c ε をさらに備える構成をとる。

宛先検査部 2 c ε は同報通信文の送信先を検査し、情報中継装置が送信先となっていて、かつ、同報通信に利用するメンバーリストが取得できる場合にのみ、同報通信文を暗号化部 2 b ε へ渡すように動作する。

この宛先検査部 2 c ε を設けることで、暗号情報作成装置 2 ε は暗号化処理だけを行うように実施でき、したがって同報通信文自体の作成は、汎用的なメッセージ作成装置（ワードプロセッサや、メーラー、チャットクライアント等）を利用できる。

例えば、暗号情報作成装置 2 ε をメーラーのプラグイン・ソフトとして実現した場合、メールの文章および添付ファイルの作成までは、既存のメーラーの機能を利用できる。暗号情報作成装置 2 ε としてのプラグイン・ソフトは、メール送信前に宛先を検査し、メーリングリスト・サーバのアドレスが宛先となっていた場合には、このアドレスに対応するメンバーリストを取得し、メンバーリストに含まれる公開鍵を利用して上述の暗号化を行い暗号情報を作成する。この暗号情報は、既存のメールが利用する通信機能（例えば、プロトコルとして S M T P を利用した通信機能）を利用して、メーリングリスト・サーバへと送信される。

なお、本実施の形態の暗号情報作成装置 2 ε に、同報通信文を作成する専用の同報通信情報作成部（図示せず）をさらに備えてもよい。

#### [第 5 - 3 b の実施形態]

次に、暗号情報作成装置 2 ε の第 5 - 3 b の実施の形態は、図 5 7 に示すように第 5 - 1 b または第 5 - 2 b の実施の形態に複数パーツ送信部 2 d ε をさらに備える構成をとる。

本実施の形態では、暗号化部 2 b ε は、同報通信文が複数のパーツで構成されている場合には、個々のパーツごとに前述の暗号化処理を行い暗号

情報を作成する。そして、複数パーツ送信部 2 d ε は、図 5 9 に示すように同報通信文が複数のパーツで構成されている場合、情報中継装置の受信能力に応じてパーツのうちのいくつかを情報中継装置から参照できる情報保管装置 5 ε に送信するように動作する。この際、各パーツの送信に最適なプロトコルを用いることができる。例えば、音声チャットには、リアルタイム通信プロトコル、ファイルの転送には、ファイル転送プロトコルを利用する。

なお、複数パーツ送信部 2 d ε は、ネットワーク上に配置されたリソースデータベースまたは、情報中継装置 4 ε に問い合わせることで、情報中継装置 4 ε から参照でき同報通信文の一部を転送しても良い情報保管装置 5 を知る。また、別の方法として、メンバーリストに情報保管装置 5 ε のアドレスを含め利用してもよい。

また、複数パーツを別々の装置に送信する場合には、受信者は、もとの情報が全部揃ったかどうかを検証する必要がある場合がある。その場合には、それぞれの暗号化処理を行なった際に、もとの全平文パーツもしくは、全暗号文パーツもしくは、各平文パーツのメッセージダイジェストの集合もしくは、各暗号文パーツのメッセージダイジェストの集合のうち一つもしくは、いくつかを組み合わせた情報に対してハッシュ関数を利用して作成したメッセージダイジェストもしくは、このメッセージダイジェストにデジタル署名したものを添付することにより、各情報をまったく異なる装置に転送した場合でも、同報通信文全体の完全性を検証することができる。

本実施の形態では、各パーツの複数のプロトコルにまたがる通信となっても、情報の暗号化処理およびメンバーリストは同一のものを利用し、確実にチームマスターが設定したメンバー間での同報通信が行え、各パーツ

の同報通信の安全性、確実性のレベルを等しくすることができる。

本実施の形態は、同報暗号通信システムにおいて、異なるフォーマットのメッセージを同時に同報通信する場合に有効である。例えば、音声チャット同報通信システムを利用して、複数の企業にまたがるメンバーが商談を行いながら、同時に、契約書ファイルを転送する場合や、メーリングリスト同報通信システムを利用して、メンバーに対して暗号メールを送信するとともに、メールシステムの許容量を超えるような大きなファイル（例えば、5 M b y t e の画像ファイル）を転送する場合がある。例えば、音声チャットの場合には、契約書ファイルを転送しようとした時点で、音声チャットの音声途切れてしまい同報通信が不通となるようでは、重要な機密情報を取り扱っている場合には、聞き落とし等が発生する危険性がある。

また、メーリングリスト同報通信装置では、それぞれの受信側メールシステムの設定によって許容量（例えば、メンバーAのシステムでは、3 M b y t e、メンバーBのメールシステムでは、1 M b y t e）が異なる上、特定メンバー用に確保されたメール受信用のバッファにどの程度空き容量あるかによって、受信能力が異なるため、送信者は、確実に送信できるか想定しがたい。本実施の形態は、これらの環境においても有効に機能するものである。

また、暗号化時に利用するメンバーリストに含まれる公開鍵は、暗号化に利用する前に有効性を検証する方がより、セキュリティの安全性が向上する。例えば、チームマスターがメンバーリストを作成した時点では、すべての公開鍵が有効であっても、一定期間後同じ鍵を使おうとしても、使

用期限を迎えた鍵が存在したり、秘密鍵が漏洩している可能性がある。暗号情報作成装置 2 ε の各実施の形態では、メンバーリスト管理装置 1 ε の公開鍵やデジタル署名に利用される秘密鍵の有効性を検証する機能と同様の鍵有効性検証機能を備えることによりさらに安全性が向上する。

以上、本発明の暗号情報作成装置の各実施の形態を説明した。

次に、本発明の暗号情報復号化装置の実施の形態を説明する。図 60 は、本発明の暗号情報復号化装置の第 5-1 c から第 5-5 c の実施の形態を包含し表している。

#### [第 5-1 c の実施形態]

暗号情報復号化装置 3 ε の第 5-1 c の実施の形態は、後述する情報中継装置から転送されてきた暗号情報を取得する暗号情報取得部 3 a ε と、暗号情報を復号化する復号化部 3 b ε とから構成される。

復号化部 3 b ε は、図 58 に示すようにまず暗号情報に含まれる鍵選択情報を参照しメンバー数に相当する複数の暗号化鍵の中から復号化に使用する暗号化鍵を選択する。そして暗号化鍵を公開鍵暗号方式を利用して受信者の秘密鍵を用いて復号化し共通鍵を得る。そして、共通鍵暗号方式を利用して、共通鍵を使用し暗号情報に含まれる暗号文を復号化し、平文の同報通信文を得る。そして、デジタル署名を送信者の公開鍵で復号化したメッセージダイジェスト MD ε と、暗号文を復号化した同報通信文（平文）をハッシュ関数で圧縮したメッセージダイジェスト MD' ε を比較・検証し、改竄や送信者の確認を行なう。

#### [第 5-2 c の実施形態]

次に、暗号情報復号化装置 3 ε の第 5-2 c の実施の形態として、図 6

0に示すように第5-1cの実施の形態の暗号情報復号化装置に、さらに受信者本人が受信したことを確認するための受信通知を情報中継装置に発信する受信通知発信部3cεを備える構成をとる。受信通知発信部3cεは、例えば、受信した通信内容のメッセージダイジェストと受信した時間のタイムスタンプ、受信者のID等に対してデジタル署名を添付した受信通知を発信する。

この構成をとるのは、例えば、受信側の端末が故障していたり、通信回線が不通となっていた場合には、通信内容が受信者に着信しない可能性がある。そのため、受信者は受信通知を発信することが望ましい。しかし、従来の受信通知（例えば、Eメールの開封通知）では、途中で悪意ある者が、成りすまして同様の通知を送ることが可能となるため、安全な受信通知とは言えない。本実施の形態の暗号情報復号化装置3εは、上記受信通知発信部3cεを設けている。これにより機密情報を送受する同報通信において、受信者本人がデジタル署名を添付した受信通知を情報中継装置に発信することができ、情報中継装置ではこのデジタル署名を検証することにより、メンバーリストに登録されたメンバーの1人に確実に配信できたことを確認できる。

#### [第5-3cの実施形態]

次に、暗号情報復号化装置3εの第5-3cの実施の形態として、図60に示すように第5-1cまたは第5-2cの実施の形態の暗号情報復号化装置に、さらに複数パーツ受信部3dεを備える構成をとる。

複数パーツ受信部3dεは、図59に示すように同報通信文の内容より、情報保管装置5εにパーツの一部分が転送されているか判断し、もし、パーツが転送されている場合、情報保管装置5εに問い合わせ、各パーツの

送信に最適なプロトコル（例えば、HTTPプロトコルやFTPプロトコル）を利用してパーツを取得する。また、本実施の形態の復号化部 3 b ε は、暗号化情報が複数のパーツで構成されている場合には、個々のパーツごとに復号化処理を行うように動作する。

なお本実施の形態は、同報通信文が複数のパーツで構成され、前述の暗号情報作成装置 2 ε により、パーツのうちのいくつかが情報中継装置 4 ε から参照できる情報保管装置 4 ε に送信される場合に対応するものである。

#### [第 5 - 4 c の実施形態]

本発明の暗号情報復号化装置の第 5 - 4 c の実施の形態は、図 6 0 に示すように第 5 - 1 c ないし第 5 - 3 c の実施の形態のいずれかの暗号情報復号化装置 3 ε に、さらに同報通信安全性検証部 3 e ε を備える構成をとる。

同報通信安全性検証部 3 e ε は、その機能の 1 つとして送信者がメンバーリストに登録されているメンバーかどうかを検証するように動作する。この検証の際には、後述のリスト取得保存部 3 f ε よりメンバーリストを取得して送信者を確認する。また、ネットワーク上に配置されたメンバーリストに関する情報を登録したリソースデータベースにアクセスし（例えばLDAPなどのプロトコル）を利用して、メンバーリストの中に含まれている送信者かどうかを、問い合わせるようにしてもよい。また、後述の情報中継装置に備わる同報通信安全性検証部と同様の機能をさらに備えてもよい。

#### [第 5 - 5 c の実施形態]

本発明の暗号情報復号化装置の第 5 - 5 c の実施の形態は、図 6 0 に示すように第 5 - 1 c ないし第 5 - 4 c の実施の形態のいずれかの暗号情報

復号化装置 3 ε に、さらにリスト取得保存部 3 f ε を備える構成をとる。

リスト取得保存部 3 f ε は、メンバーリストをネットワーク上に配置されたリソースデータベースに保存されたメンバーリストを、同報通信と同じ、または、異なるプロトコル（例えば、同報通信で S M T P を利用する場合には、H T T P など）を利用して取得する。もしくは、転送されてきたメンバーリストを記憶装置（図示せず）に保存し、必要なときに保存先からメンバーリストを読み込むことにより取得する。

また、暗号情報復号化装置 3 ε がすでにメンバーリストを保存している場合には、リスト取得保存部 3 f ε は、メンバーリストが最新バージョンか確認するように動作する。例えば、メンバーリストの最新バージョンに関する情報が保存されたネットワーク上に配置されたデータベースに、同報通信と同じまたは、異なるプロトコル（例えば、同報通信で S M T P を利用する場合には、L D A P、O C S P など）を利用して、最新のメンバーリストのバージョンを問い合わせ確認する。

また、リスト取得保存部 3 f ε は、前述のメンバーリスト管理装置 1 ε の実施の形態で説明したメンバーリストの正当性を検証する機能を備え、メンバーリストの取得時にメンバーリストの正当性を検証する。

さらに、前述の暗号情報作成装置の実施の形態で説明した公開鍵やデジタル署名に利用される秘密鍵の有効性を検証する機能を、復号化部 3 b ε、リスト取得保存部 3 f ε に備え利用する形態としてもよい。これらの機能をさらに備えることで、安全性がさらに向上する。

以上、本発明の暗号情報復号化装置の各実施の形態を説明した。

図 6 1 は、本発明の情報中継装置の第 5 - 1 d から第 5 - 6 d の実施の



形態を包含し表している。

[第5-1dの実施形態]

まず、本発明の情報中継装置の第5-1dの実施の形態を説明する。

本実施の形態は、チームマスターによって管理される配信先リストを保存・管理する配信先リスト管理部4aεと、転送されてきた暗号情報を、配信先リストに含まれる被配信メンバーに転送するために複製する情報複製部4bεと、複製された暗号情報をそれぞれの被配信メンバーに送信する送信部4cεとから構成される。

配信先リスト管理部4aεは、配信リストを保存・管理する機能と、メンバーリストを取得し保存する機能と、メンバーリストを取得する際に、メンバーリスト管理装置の実施の形態で説明したメンバーリストの正当性を検証する機能と、メンバーリストと配信リストに含まれるメンバーを一致させる機能を備える。なお、配信先リスト管理部4aεがメンバーリストを参照して配信先リストを設定する場合には、メンバーリストが最新バージョンであるか確認する機能をさらに備える。例えば、メンバーリストの最新バージョンに関する情報が保存されたネットワーク上に配置されたデータベースに、同報通信と同じまたは、異なるプロトコル（例えば、同報通信でSMTPを利用す場合には、LDAP、OCSPなど）を利用して、最新のメンバーリストのバージョンを問い合わせるようにしてもよい。

[第5-2dの実施形態]

本発明の情報中継装置の第5-2dの実施の形態は、第5-1dの実施の形態の情報中継装置4εに、リスト正当性確認部4dεをさらに備える構成をとる。

リスト正当性確認部 4 d ε は、メンバーリストを取得した場合に、メンバーリスト正当性の検証を行う。このメンバーリストの正当性の検証を行なう機能は、前述のメンバーリスト管理装置 1 ε の実施の形態で説明したとおりである。

#### [第 5 - 3 d の実施形態]

本発明の情報中継装置の第 5 - 3 d の実施の形態は、第 5 - 1 d または第 5 - 2 d の実施の形態の情報中継装置 4 ε に、付加情報添付部 4 c ε をさらに備える構成をとる。

付加情報添付部 4 c ε は、チームマスターまたは情報中継装置 4 ε の管理者による各種情報（サービス情報、管理情報等）を暗号情報に添付するものである。この付加情報を添付する機能により、被配信メンバーに幅の広いサービスを提供することができる。

#### [第 5 - 4 d の実施形態]

本発明の情報中継装置の第 5 - 4 d の実施の形態は、第 5 - 1 d ないし第 5 - 3 d の実施の形態のいずれかの情報中継装置 4 ε に、同報通信安全性検証部 4 f ε をさらに備える構成をとる。

同報通信安全性検証部 4 f ε は、第 1 の機能としてメンバーリストの同一性を検証する機能をもつ。例えば、送信側の端末が故障していたり、通信回線が不通となっていた場合には、最新のメンバーリストが送信者に行き渡っていない可能性がある。同報通信安全性検証部 4 f ε は、より同報通信の安全性を高めるために、転送されてきた暗号情報の暗号化時に利用したメンバーリストと、サーバが転送時に利用する配信先リストを作成するために用いたメンバーリストとの同一性の検証を行う。

例えば、メンバーリストのバージョンNoやチームマスターがメンバーリストを作成したときの時間（例えば、タイムスタンプなどが付加されていた場合）などの情報を利用して、メンバーリストが同一のものを検証することができる。また、別の手法としては、メンバーリストに添付されたデジタル署名者が同一かどうかを検証することにより、同一性検証を行うことができる。また、別の手法としては、メンバーリストに対してハッシュ関数を利用してメッセージダイジェストを比較することにより、同一性検証を行うことができる。

また、同報通信安全性検証部4fεは、第2の機能として同報通信送信者を検証する機能をもつ。従来の同報通信は、情報中継装置4εの管理者が情報の中身を見ることができたため、例えば、中傷・誹謗情報が流れているか否かなどの、内容を検査することができた。しかし、本発明の方式では、サーバの管理者が情報の中身を見れない仕組みを実現しているため、この情報中継装置4εを不正に利用される可能性がある。そこで、同報通信安全性検証部4fεは、情報受信を拒否する情報端末（例えば、IPアドレスなどによって識別できる）、または、利用者の識別情報（例えば、メールシステムの場合には、メールアドレスや、信頼できる認証局より発行された証明書などによって識別できる）が含まれる受信拒否情報を取得し、情報中継装置4εに転送されてきた情報の送信者または、送信端末が、受信拒否情報に含まれているか否かを検証する機能をもつ。なお、受信拒否情報には、例えば、過去にスパムメールを発した個人のメールアドレスや、セキュリティレベルが低く本人識別が正当な手順をもって行われていない可能性がある端末のIPアドレスやネットワークアドレスのリストが含まれている。

また、同報通信安全性検証部 4 f ε は、第 3 の機能として同報通信内容を検証する機能をもつ。これは、同報通信の安全性を高めるために、送信者や通信内容についても検証を行なうものである。暗号情報の送信者がメンバーリストに含まれた者かどうかの検証や、転送されてきた情報の中に悪意あるプログラムやデータ列が含まれているかどうかの検証を行なう。

また、同報通信安全性検証部 4 f ε は、第 4 の機能として複数パーツからなる暗号情報のうち、情報保管装置に保存され暗号情報復号化装置から参照されるパーツが間違いなく情報保管装置に転送されたかを検証する機能をもつ。転送されてきた暗号情報を参照して複数のパーツで構成される暗号情報のうち、一部を別の情報保管装置に転送しているか判別し、一部が別の情報保管装置に転送されている場合、確実に転送されたかを検証する。

さらに、前述の暗号情報作成装置の実施の形態で説明した公開鍵やデジタル署名に利用される秘密鍵の有効性を検証する機能は、同報通信安全性検証部 4 f ε に備えられ利用される形態もある。

#### [第 5 - 5 d の実施形態]

本発明の情報中継装置の第 5 - 5 d の実施の形態は、第 5 - 1 d ないし第 5 - 4 d の実施の形態のいずれかの情報中継装置 4 ε に、同報通信内容保存部 4 g ε をさらに備える構成をとる。

同報通信内容保存部 4 g ε は、転送されてきた情報、または、情報の一部、または、それらの情報に添付情報を添付して保存する。例えば、メールシステムにおけるメールサーバに障害が発生した場合や、受信者の端末が故障していた場合には、送信された情報であっても正確に受信されない

可能性がある。また、音声チャットにおいて通信回線の都合上、音声が途切れ途切れになる場合などもある。このように送信側が送ったデータと受信側が受け取ったデータが一致しなかった事態が発生しても、同報通信内容保存部 4 g ε による保存機能により安全に保存しておき、必要になったときに再度確認したり再取得することができる。

[第 5 - 6 d の実施形態]

本発明の情報中継装置の第 5 - 6 d の実施の形態は、第 5 - 1 d または第 5 - 5 d の実施の形態のいずれかの情報中継装置 4 ε に、同報通信自動開設部 4 h ε をさらに備える構成をとる。

同報通信自動開設部 4 h ε は、同報通信をサーバ管理者の手動の許可を得ることなく自動的に開始するため、サーバ管理者が開設受付の際に開設要求者が満たすべき項目を提示するための開設要求項目提示機能と、開設要求者が転送してきた開設受付要求が、開設要求項目を満たし、開設を許可するか否かを判断する開設許可判断機能と、開設が決定されると、開設要求者をチームマスターとし、チームマスターが指定したメンバーに同報通信が可能になるよう開設設定を行う同報通信開設設定機能をもつ。

従来の同報通信システムは、事前に情報中継装置の管理者が、開設に伴う作業を行う必要があった。例えば、配信リストの設定や、I C カードを配布したり、情報中継装置に公開鍵を登録したりする作業が必要であった。また、暗号同報通信は、延々と続く通信ではなく、例えば、1 時間の音声チャット、3 通の契約書ファイルの転送といったように、必要なときに最小限の時間で利用する通信であることも多いと考えられる。その場合、情報中継装置 4 ε の同報通信の開始や削除に関する作業負担が非常に大きくなる。また、ミスの発生や悪意のある管理者の存在などの危険性があるた

め、このような人による手動の設定はできるだけ必要としないシステムが、安全上望ましい。そこで、本実施の形態の情報中継装置 4 ε は、サーバ管理者の手動の設定を必要とすることなく、一定の利用条件（例えば、利用時間に比例する料金の支払い等）を満たせば、自動的に同報通信を開始できる機能を提供する。

さらに、同報通信自動開設部 4 h ε は、開設要求者が転送してきた開設受付要求が、正確な要求であるかどうかを検証する開設要求確認機能を備えてもよい。例えば、課金項目にクレジットカードが記されていた場合に、クレジットカードの番号がきちんと登録され課金可能な状態であるかを検証する。この検証の際に、情報中継装置 4 ε に検証に利用するデータが無い場合には、ネットワーク上に配置され所定のデータをもつデータベースやサーバ等に問い合わせる。

第 5 - 6 d の実施の形態の情報中継装置 4 ε に、同報通信のメンバーの脱退要求を受け付ける脱退要求受付部（図示せず）を備えてもよい。

例えば、加入する意志がないのに、勝手にメンバーリストに登録されて、不要な情報や中傷・誹謗情報ばかりが転送されるという危険性がある。本形態の情報中継装置 4 ε では、脱退要求受付部は、同報通信のメンバーが、情報中継装置に対して同報通信から脱退するという脱退要求が来た場合には、該メンバーへの転送をとりやめ、その故をチームマスターに連絡する脱退要求受付部を備える。また、脱退要求が、間違いなく脱退要求メンバー本人が作成した転送中止要求かどうかを調べるために、デジタル署名やシェイクハンドなどの本人確認手法を利用することができる。

以上、本発明の情報中継装置の各実施の形態を説明した。

次に、本発明の同報通信システムの実施例 5-1 として、第三者が運用する情報中継装置を利用して、証券会社が証券ニュースを会員に配信する例を説明する。図 6 2 に示す実施例 5-1 では、メールシステムの安全な同報通信を実現するため、メーリングリスト・サーバと WWWサーバを用いて本発明の情報中継装置の機能を実現している。このメーリングリスト・サーバが第三者によって運用されている。

第三者が運用するメーリングリスト・サーバと連動した WWWサーバで、WWWサーバには、同報通信の開設にメーリングリスト・サーバの管理者が設定した、開設要求者が満たすべき項目を示したホームページが保存されている。証券会社は、サービスを自動開設するために、SSL (Secure Socket Layer) 通信を利用してこのホームページをダウンロードし、ブラウザに表示された項目に対応するフォーム内に必要事項を入力する。本実施例 5-1 では、名前、クレジットカード番号と 1000 人まで同報通信できるサービスを要求することを記載して、送信ボタンを押し、WWWサーバに転送する。

WWWサーバ上で稼動するプログラム（例えば、CGI）として実装された同報通信自動開設部 4 h ε の開設許可判断機能は、SSL 通信で確認したアクセスした者の証明書と、名前、クレジットカード No、「1000」の 4 つデータを利用して、開設を許可すべきか否かを判断する。実施例 5-1 では、クレジットカード No をクレジットカードサービス会社に問い合わせ、カード保持者と証明書の所有者が一致するかどうかを検証し、一致した場合には、開設を許可する旨を知らせるページを加入要求者に再度転送する。一致しない場合には、開設が拒否された旨を知らせるページを加入要求者に再度転送する。

開設を許可した場合には、メーリングリストサーバ上で稼動するプログラムとして実装された同報通信自動開設部 4 h ε の同報通信開設設定機能により、加入要求者がチームマスターとなって管理する同報通信のためのメーリングリストアドレスを新規に設定する。また、このメーリングリストアドレスに送信されてきた情報を配信するための配信リスト（当初は、空のリスト）を設定する。これらの開設設定が終了するとメーリングリストサーバは、チームマスターに対して、開設設定が成功終了した旨を通知するメールを転送する。

実施例 5 - 1 におけるメンバーリスト管理装置 1 ε は、例えば J A V A のアプレットとして実装され、ホームページのなかに組み込まれて、W W Wサーバに保存されている。チームマスターは、メンバーリストを作成する際に、S S L通信を利用してダウンロードされてくるアプレットを用いて、設定したいメンバーリストの管理を行う。本実施例 5 - 1 におけるメンバーリストは、チームマスターリスト、レポーターリスト、受信者リストの 3 つのリストで構成されている。チームマスターリストには、チームマスター以外にチームを管理できるサブマスターを設定し、レポーターリストには、証券ニュースを書く記者を登録し、チームマスターのデジタル署名を行って、情報中継装置 4 ε に再度転送する。情報中継装置 4 ε は、メンバーリストが間違いなくチームマスターによって作成されているかをデジタル署名を検証した後、配信リストを設定する。本実施例 5 - 1 での配信ルールは、レポーターリストのメンバーから転送されてきた同報通信情報を受信者リスト（メンバーリストに含まれる）に登録されたメンバー分複製し、登録するように設定されている。



受信者は、基本的に毎月の課金が行えるユーザであれば自動的に加入してもらえよう実装するため、本実施例 5-1 では、メンバーリスト管理部 1 の加入要求受付部 1 d ε を利用する。チームマスターによって設定されたメンバーリストに含まれるチームマスターリストには、複数のサブマスターが設定されている。サブマスターもまた、証券会社の社員であり、このサブマスターは、受信者リストの管理を担当している。サブマスターは、WWW のページとして実装された加入要求受付部 1 d ε の加入要求項目設定機能を、SSL 通信を利用してダウンロードする。この際、WWW サーバは、SSL 通信で取得できるサブマスターの証明書を見て、サブマスター本人の識別・認証を行う。WWW ページ内のフォームの各項目を埋めていくことによって、加入要求項目を設定する。本実施例では、サービスの契約同意書、課金項目、メールアドレスとメールアドレスを含む証明書を提示してもらう旨を指定し、さらに、加入要求者の加入要求を暗号化するためのサブマスターの公開鍵を指定して転送する。

上記証券ニュース配信サービスへの加入要求者は、WWW ページに埋め込まれた J A V A アプレットとして実装された加入要求受付部 1 e ε の加入要求項目提示機能を利用して、まず、契約同意書に自分の秘密鍵を利用してデジタル署名を行い、また、課金項目、メールアドレスを入力する。これを転送する際には、これらの機密情報（特に、課金に関する情報：クレジットカード N o や銀行の口座番号等）は、WWW サーバやメーリングリストサーバの管理者に見えてはいけなないので、サブマスターの公開鍵を取得して暗号化を行ってから、WWW サーバに転送する。また、以上の通信は、SSL で行われているため、認証を行う際に証明書も確認することができる。

多数の加入要求者からの加入要求は、WWWサーバに暗号化された加入要求情報として保存されている。実装例 5-1 では、加入要求受付部 1 e ε の加入許可判断機能を実装したプログラムは、WWWサーバにアクセスし、暗号化された加入要求情報を取得し、各項目がサービス加入を許可できるよう満たされているかどうかを判断する。例えば、鍵有効性検証機能を利用して、公開鍵と秘密鍵がまだ有効であるかを検証する。判断の結果、加入を許可または、拒否した旨を示す通知メールを加入要求者に対して転送する。このプログラムは、さらにメンバーリスト管理装置を自動操作することができる。

許可が出された加入要求に対しては、メンバーリスト管理装置 1 ε を利用して、WWWサーバに保存されたメンバーリストを、メンバーリスト取得保存部 1 c ε を利用して取得し、メンバーリストのうち、受信者リストに加入要求者を登録する。このメンバーリストには、サブマスターとして登録されているサブマスターの秘密鍵を用いてこの受信者リストに対してデジタル署名を添付し新メンバーリストとして、再度WWWサーバに転送する。WWWサーバでは、前述のメンバーリストの正当性を検証する機能を利用してメンバーリストの正当性を確認し、さらに公開鍵やデジタル署名に利用される秘密鍵の有効性を検証する機能を利用してメンバーリストに含まれている公開鍵がすべて有効であるかを検証する。これらの検証結果が肯定であれば、配信先リスト管理部 4 a ε を利用して配信先リストを更新する。また、レポーターリストに含まれているメンバーに対しては、最新のメンバーリストをリスト送信部 1 d ε（実施例では、SMTP プロトコルを利用して実装されている）を利用して、送信しておく。

記者が証券ニュースを作成する端末は、汎用的なコンピュータ（本実施

例 5-1 では、ノートブックパソコン等) などに、電子メールソフトウェアが組み込まれている。この電子メールソフトウェアを利用して作成した記事をメーリングリストのアドレスを指定して転送しようとする。この時、この電子メールソフトウェアと連動するプラグイン・ソフトウェアとして実装された暗号情報作成装置 2 ε は、宛先検査部 2 c ε を利用して、メーリングリストアドレスがメンバーリストの存在する情報中継装置 4 ε に転送しようとしていることを確認する。

この場合、プラグイン・ソフトウェアは、まず、リスト取得保存部 2 a を利用して、端末のパソコンに存在するメンバーリストのバージョンが最新のバージョンかを検証する。これは、ネットワーク上に X. 500 の標準に基づいて構築されたリソースデータベースに対して最新のバージョンを、LDAP を利用して問い合わせる。最新のバージョンでなかった場合には、リソースデータベースに登録された最新バージョンの所在場所から最新のメンバーリストを取得する（実施例では、WWWサーバより、SSL 通信を利用して取得する）。

暗号情報作成装置 2 ε では、メンバーリストの正当性を検証する機能を利用してメンバーリストの正当性を確認後、メンバーリストに含まれる受信者リストのメンバーの公開鍵を利用して暗号化部で、暗号化を行う。この際に、デジタル署名付加機能は、記者が保有する秘密鍵を記録した IC カードから、この記者の秘密鍵を取得し、作成された記事に対してデジタル署名を添付する。このデジタル署名により、受信者は、どの記者が書いた記事かを確認でき、記事の信頼性を確かめることができる。また、記事を配信した記者は、記事を作成したこと否認できなくなる。

メーリングリストのアドレスに送信されたメーリングリストは、まず、同報通信安全性検証部 4 f ε を利用して送信された情報のデジタル署名添付者（本実施例 5 - 1 では、記者）が、間違いなくメンバーリストのうちのレポーターリストに含まれているか確認する。また、メンバーリストの同一性を検証する機能を利用して、メンバーリストのバージョンが異なっていないかを検証する。検証した結果、メンバーリストのバージョンが異なる場合には、その旨を明示した情報と同報通信情報をこの記者に対して返信する。以上の検証の結果、すべて正常であれば、情報複製部 4 b ε を利用して暗号情報を複製し、メンバーリストの受信者リストに含まれるメンバーに対して、SMTP プロトコルで実装された送信部 4 c ε を利用して送信する。

受信者の電子メールソフトウェアに組み込まれたプラグイン・ソフトウェアとして実装された本発明の暗号情報復号化装置は、復号化部 3 b ε のデジタル署名を検証する機能を利用して改竄の有無および情報作成者を確認して、送信者が証券会社の記者であることを確認する。確認後記事を復号化して、記事を読むことができる。記事が無事復号化できた時点で、受信通知発信部 3 c ε を利用して、情報中継装置 4 ε に対して受信通知を送信する。

なお、本実施例における J A V A アプレットが本当に悪意がないかどうかをチェックするには、J A V A アプレットに添付されたデジタル署名を確認することによって、検証できる

以上、実施例 5 - 1 における各装置の動作を説明した。

次に、本発明の同報通信システムの実施例 5 - 2 として、複数の企業間

にまたがるメンバー間（この集合を、チーム 0 0 1 ε とする）で見積もりや商談等の機密情報を同報通信して行う場合に利用される例を説明する。図 6 3 に示す実施例 5 - 2 では、情報中継装置としてメーリングリストサーバを利用する。

チーム 0 0 1 ε のチームマスターは、汎用的なデスクトップコンピュータの OS 上に実行ファイルとして実装されたメンバーリスト管理装置 1 ε を利用して、機密情報を同報通信するメンバーリスト管理を行う。リスト取得保存部 1 c ε を利用してメンバーリストを取得し、リスト作成・変更 GUI 画面を開く。この GUI 画面には、チーム 0 0 1 ε のメンバーの一覧と、公開鍵管理部 1 b ε を利用して端末にある公開鍵のデータベースにアクセスし、保存されている公開鍵の一覧を表示している。

チーム 0 0 1 ε のチームマスターは、公開鍵一覧から、チームに加入するメンバーの公開鍵を選択し、チーム 0 0 1 ε のメンバー一覧に追加する。また、公開鍵管理部 1 b ε が提供するネットワークアクセス機能を利用して、ネットワーク上の認証局が提供するディレクトリーサービスにアクセスし、端末になかった公開鍵で新たにチーム 0 0 1 ε に追加したいメンバーの公開鍵を取得し、この公開鍵をメンバーリストに加える。

GUI 画面には、OK ボタンが表示されており、チーム 0 0 1 ε のメンバーを変更し終わったら、この OK ボタンを押す。この時点で、公開鍵やデジタル署名に利用される秘密鍵の有効性を検証する機能は、メンバーリストに含まれるそれぞれの公開鍵が含まれる証明書を発行した認証局のディレクトリーサービスに LDAP プロトコルを利用してアクセスし、この公開鍵が有効であるかどうかを検証する。検証の結果、無効の公開鍵があれ

ば、その旨をダイアログに表示して、チームマスターに通知する。すべて有効であれば、タイムスタンプと、メーリングリストのアドレスとチームIDとチームマスターの識別名で構成されるメンバーリストを作成し、このメンバーリストの全体のデータをハッシュ関数のMD5を利用して圧縮し、圧縮データを生成する。

次に、チームマスターの秘密鍵にアクセスし、チームマスターがダイアログボックスより入力したパスワードを利用したパスワード復号化（実施例では、共通鍵暗号方式RC2を利用して実装されたパスワード復号化を利用する）を行う。その結果取得した、チームマスターの秘密鍵を利用して、圧縮データを公開鍵暗号方式RSAで、暗号化することにより、デジタル署名を作成する。このメンバーリストとデジタル署名を情報中継装置4εにSMTPプロトコルを利用してメールとして転送する。

情報中継装置4εでは、配信先リスト管理部4aεのメンバーリスト取得機能を利用して、受信したマルチパート（MIME（Multipurpose Internet Mail Extensions））のフォーマットで構成されたSMTPメールの中身を解析し、Content-Typeより判断したメンバーリスト部分を抽出して、リスト正当性確認部4dεに入力する。リスト正当性確認部4dεは、メンバーリストのデジタル署名者として間違いなくチーム001εのチームマスターのデジタル署名が添付されていることを確認し、配信先リスト管理部4aεを利用して、配信先リストの受信者を変更する。その後、変更されたばかりの配信先リストの受信者に対して、メンバーリストとデジタル署名をMIMEフォーマットごと複製し、配信先リストの各受信者に対して転送する。

汎用的なデスクトップコンピュータ上にインストールされたメーラーとして動作する暗号情報作成装置 2 ε は、メンバーリストが含まれたメールを受け取った場合には、MIME の Content-Type より、このメールが同報通信におけるメンバーリストであることを識別する。その時点で、メーラーは、メンバーリストとデジタル署名を抽出し、リストの正当性を検証する機能を利用して、メンバーリストの正当性を確認した後、リスト取得保存部 2 a ε を利用して保存しておく。

チーム 001 に含まれるメンバーが、汎用的なデスクトップコンピュータ上で可動する一般的な実行プログラムとして実装された暗号情報作成装置 2 ε の同報通信情報作成機能を利用して、見積書と契約書の 2 つの添付ファイルを含むメールを作成した後、送信ボタンを押すと、宛先検査部 2 c ε が送信先アドレスをチェックし、送信先アドレスが端末に保存されている複数メンバーリストのうち、送信先アドレスのために私用するメンバーリストがあるかを検査する。

メンバーリストがあった場合には、この添付ファイルとメールを、メンバーリストの公開鍵を利用して暗号化する。その際に、暗号化部 2 b ε は、それぞれの添付ファイルとメール本文を別々に暗号化し、デジタル署名も個々に添付する。これらの複数のパーツで構成された情報の内、添付ファイルはそのまま添付せずに、情報保管装置（情報保管サーバ） 5 ε に転送する。複数パーツ送信部 2 d ε は、情報中継装置 4 ε のアドレスをもとに、メーリングリストアドレスに対応する情報保管装置 5 ε をネットワーク上のデータベースに問い合わせ、2 つの添付ファイルを送信すべき情報保管装置 4 ε のアドレスと、送信方法（例えば、プロトコルなど）を特定する。

情報保管装置 5 ε は、H T T P プロトコル利用したファイル転送を許可する仕組みであることが分かると、H T T P プロトコルを利用して送信する。その際に、情報保管装置 5 ε は、S S L 通信を利用しユーザ認証が可能であるため、ユーザがメーリングリストサーバで行っている同報通信サービスを利用しているメンバーリストに含まれているかを確認することができる。メール本文は 2 つの添付ファイルの送信とは別に、情報保管サーバのアドレスを添付してアドレスを転送する。

メーリングリストのアドレスに送信されたメーリングリストは、まず、同報通信安全性検証部 4 f ε を利用して送られてきた情報のデジタル署名添付者が、間違いなくメンバーリストのうちのレポーターリストに含まれているか確認する。また、メンバーリストの同一性を検証する機能を利用して、メンバーリストのバージョンが異なっていないかを検証する。検証の結果、メンバーリストのバージョンが異なる場合には、その旨を明示した情報と同報通信情報を記者に対して返信する。また、同報通信安全性検証部 4 f ε の同報通信内容検証機能を利用し、通信内容の中に、装置やソフトウェアのバグを利用した悪意あるプログラムやウィルスなどが含まれていないかを検証する。さらに、同報通信安全性検証部 4 f ε の情報保管装置参照機能を利用して、間違いなく暗号化された 2 つ添付ファイルが情報保管装置 4 ε に転送されて保存されているかを検証する。

以上の検証の結果、すべて正常であれば、同報通信内容保存部 4 g ε を利用し、同報通信の内容をメーリングリストサーバに接続されたデータベースに保存しておく。その際に、タイムスタンプとメーリングリストサーバの秘密鍵を利用したデジタル署名を添付して保存する。また、暗号情報には、情報保管装置 4 ε に添付ファイルが保存されていることを確認した



事に関する時間と、この暗号情報が、メーリングリストサーバに保存されている事に関する情報を添付して、情報複製部 4 b ε を利用して暗号情報と添付情報を複製し、メンバーリストの受信者リストに含まれるメンバーに対して、SMTP プロトコルで実装された送信部 4 c ε を利用して送信する。

出張先のWWWブラウザで、メールを取得しようとしているユーザは、J A V A アプレットとして実装された暗号情報復号化装置 3 ε を、ダウンロードしブラウザ上でこの暗号情報を受信する。この J A V A アプレットは、ネットワーク上よりリスト取得保存部 3 f ε を利用してメンバーリストの最新バージョンを取得し、リストの正当性を検証する機能を利用して、メンバーリストがチームマスター本人によって、作成されたものかどうかを確認する。この暗号情報を取得した際に、まず、復号化部 3 b ε のデジタル署名を検証する機能を利用して改竄・情報作成者を確認し、さらに、同報通信安全性検証部 3 e ε の送信者信頼性確認機能を利用して、メンバーリストに含まれる商談相手であることを確認する。その後、復号化部 3 b ε を利用し、情報を復号化して暗号情報を見ると情報保管装置 5 ε に添付ファイルが送信されていることが判明する。複数パーツ受信部 3 d ε は、この添付ファイルを H T T P プロトコルを利用してダウンロードし、それぞれのファイルを再度復号化し、もとの情報を得ることができる。

以上、実施例 5 - 2 における各装置の動作を説明した。

なお、本発明は、インターネットの他、LAN やダイヤルアップによるネットワークを利用してもよい。

また、本発明のメンバーリスト管理装置を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録さ

れたプログラムをコンピュータシステムに読み込ませ、実行することによりメンバーリスト管理を行ってもよい。すなわち、このメンバーリスト管理プログラムは、同報通信を行う 1 以上のメンバーの公開鍵を含むメンバーリストを作成する機能と、前記公開鍵を取得し保存する機能とをコンピュータに実現させる。

また、本発明の暗号情報作成装置を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより暗号情報作成を行ってもよい。すなわち、この暗号情報作成プログラムは、ネットワークを介して、メンバーリストを取得し保存する機能と、同報通信文を取得し、該同報通信文を前記メンバーリストに含まれる公開鍵を用いて暗号化し暗号化情報とする機能とをコンピュータに実現させる。

また、本発明の暗号情報復号化装置を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより暗号情報復号化を行ってもよい。すなわち、この暗号情報復号化プログラムは、情報中継装置から転送された暗号情報を取得する機能と、前記暗号情報に含まれる暗号化情報を復号化する機能とをコンピュータに実現させる。

また、本発明の情報中継装置を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより情報中継処理を行ってもよい。すなわち、この情報中継処理プログラムは、配信先リストを管理する機能と、転送されてきた暗号情報を複製する機能と、複

製された暗号情報を各被配信メンバーに配信する機能とをコンピュータに実現させる。

また、モバイルネットワーク環境においても同報通信を実現するため、同報通信に必要な本発明のメンバーリスト管理装置、暗号情報作成装置、暗号情報復号化装置を持たない端末を利用しなければならない場合でも、この端末にネットワーク上に配置され各装置のそれぞれの機能を実現するソフトウェアを保存しているソフトウェア保管装置から、各装置の機能を実現するソフトウェアをダウンロードして、端末に内蔵されたコンピュータシステムに読み込ませ実行させることにより、同報通信を行なってもよい。

以上詳細に説明したように、第5-1a～5-4a，第5-1b～5-3b，第5-1c～5-5c，第5-1d～5-6dの実施形態の発明によれば、以下の効果がある。

本発明によれば、情報中継装置において暗号化された情報を復号化しない仕組みとしたので、情報中継装置の管理者による同報通信の通信内容の漏洩や改竄等の不正を防ぎ、本当に情報を共有する必要のあるメンバーにだけ同報通信内容を共有することができる。

また、本発明によれば、メンバーリスト管理部に加入要求受付部を、そして情報中継装置に同報通信自動開設部を設けたので、同報通信を行う受信者の脱退や、加入に対して迅速に対応でき、同報通信メンバーの動的な変更があっても、誤って同報通信してはいけないメンバーに情報を転送してしまうことを防止できる。

また、本発明によれば、メンバーリストによる管理を行なうので、情報中継装置の管理者が同報通信の被配信メンバーを管理するのではなく、同

報通信を行うメンバーの中で被配信メンバーを管理でき、さらにメンバーの管理者に集中する管理負担を軽減することができる。

また、本発明によれば、情報中継装置において同報通信安全性検証部および同報通信内容保存部を設け、暗号情報復号化装置において受信通知発信部および同報通信安全性検証部を設けたので、多数の被配信メンバーそれぞれが、情報を確実に受信できる。

#### [第6の実施形態]

第6の実施形態の発明は、企業の部や課といった組織単位に相当するチームの構成員（ユーザないしメンバ）間で各種の情報やユーザに提供される様々な機能を共有するためのチームデータリストを作成、管理、保管し、それによって、これら情報や機能をユーザ間でチーム毎に安全に共有してゆくためのチームデータリスト処理システムに関するものである。さらに詳細には、チームデータリストの保管に係わる処理を担うチームデータリスト保管装置と、チームデータリスト保管装置から取得したチームデータリストを対象として様々な管理を行うチームデータリスト管理装置を備えたシステムに関するものである。

第6の実施形態の発明に関し、従来以下説明する技術が知られている。

ユーザに提供される各種の情報や機能といった様々な資源を複数のユーザ間で共有するためには、これら資源にアクセスを要求しているユーザが、本当に資源へアクセスする権利を有しているのか否かを検証する機能を用意しておく必要がある。かかる検証を行うために、従来は、資源に対する正当なアクセス権限を付与されたユーザを予め定義したアクセスコントロールリスト（以下、「ACL」と略記する）と呼ばれるリストを利用している。なお、ここで言うACLは、上述したチームデータリストに含まれ

る種々の情報のうち、共有資源に対するアクセスを制御するための情報だけが含まれたリストの一例である。

図 7 6 は、A C L を利用して複数のユーザ間で情報共有を行う従来のシステムの概要を示したものである。同図に示されるシステムでは、イントラネット 1 と、インターネット 2 とがそれぞれファイアウォール 3 と、4 とを介してサーバ 5 とに接続されており、イントラネット 1 内部の者ばかりでなく、イントラネット外の共有メンバ 6 とがインターネット 2 とを介して互いに情報を共有している。周知のように、イントラネット 1 とは企業内に整備されたネットワークなどの閉じたネットワークであり、その一方で、インターネット 2 は世界中にまたがるパブリックなネットワークである。

また、ファイアウォール 3 と、4 とは悪意を持った侵入者などがイントラネット 1 とへ不正にアクセスすることを防止するためのコンピュータである。サーバ 5 とは各種の資源が蓄積されている端末（コンピュータ）であって、共有情報が格納されたデータベース 7 と、特定の情報ないし機能にアクセスしても良いグループ及びそれに属するメンバのメンバリストを保持した A C L 8 とを備えている。このサーバ 5 とは、データベース 7 とに蓄積されている共有情報を管理するデータ保管機能のほか、クライアントに相当する通信相手が予め許可されている者か否かを検証するユーザ認証機能、A C L 8 とに基づいて共有情報に対するアクセスの可否を検証するアクセス制御機能、A C L 8 とに基づいて特定のグループに属するメンバだけが特定の共有情報へアクセスすることを可能ならしめるグループ管理機能を備えている。

図 7 6 のシステムでは、共有メンバ 6 とやイントラネット 1 と内部のユーザからデータベース 7 とに対するアクセス要求があると、サーバ 5 とはその都度 A C L 8 とを参照してユーザ認証を行い、当該ユーザがメンバとして A C L 8 とに定義されていればアクセスを許可し、メンバとして定義されていなければアクセスを拒否する。また、当該ユーザに対してアクセスが許可されている場合、サーバ 5 は A C L 8 とを参照して当該メンバが特定のグループに含まれるかどうかを確認するとともに、当該メンバがアクセス要求のある共有情報に関してアクセスを許されているかどうか調べるようにしている。

一方、図 7 7 は特定グループに属するメンバだけで情報を共有するための従来の一実現例を示したものであって、図中のサーバ S V とは図 7 6 のサーバ 5 とに対応し、クライアント C L とは図 7 6 の共有メンバ 6 とやイントラネット 1 と内部の者が操作する端末である。図 7 7 では、サーバ S V と上にメンバーリスト 9 とを設けている。グループ毎に存在するメンバーリスト 9 とは、当該グループに付与されている識別子であるグループ I D、グループ内の各メンバの公開鍵、これら公開鍵に付与されている識別子である公開鍵番号（図中の公開鍵 N o）で構成されており、当該グループのチームマスターのデジタル署名が付されている。

クライアント C L とがグループ I D を指定してある特定のグループに関するメンバーリストをサーバ S V とに要求すると、サーバ S V とは所定の権限確認を行ったのちに、指定されたグループ I D に対応するメンバーリスト 9 とを公開鍵 I D リストとしてクライアント C L とに転送する。クライアント C L とは当該リストに含まれるチームマスターのデジタル署名が正当なものであることを確認したのち、送られたメンバーリストをグルー

ブに対するメンバの加入，退会などに応じて当該メンバの公開鍵及び公開鍵IDを追加，削除することによってメンバーリスト9aをを作成する。次いで、クライアントCLはメンバーリスト9aにデジタル署名を行い、サーバSVにメンバーリスト更新要求を行ってメンバーリスト9aを返送する。これにより、サーバSVは所定の権限確認を行ったのち、クライアントCLからのメンバーリスト9bを受け取ってサーバSV上のグループの更新処理を行う。

ところで、複数のユーザ間で資源を共有する場合にはサーバ側の管理者を共有メンバに含めるのが好ましくない場合もある。例えば、ある企業の情報システム部に所属するシステム管理者は、人事部内だけで共有すべき企業の人事情報にアクセス不可能であることが必要と考えられる。ところが、上述した図76のようなシステムや図77の処理手順では、サーバ5やサーバSVの管理者に対してACL8の設定や管理を行う権限を許与してしまっている。そのため、これらサーバ管理者はACL8に対して不正なアクセスを行うことが可能であり、意図的にACL8の設定内容が改竄されるのを防止することができない欠点がある。これに加えて、サーバ管理者以外にも、サーバSVへ不正に侵入する者（いわゆるクラッカ）によってACL8が不正に改竄されてしまうおそれもある。

また、上述したような従来のシステムでは、限られた少数のサーバ管理者に権限の設定を行ってもらう必要があるため、こうした権限設定作業に関わる負担がこれら少数の管理者に集中してしまうという問題もある。しかも、イントラネット内部でだけ情報を共有するような形態であればまだしも、例えば企業のシステムを企業外の第三者に委託して運営させるような利用形態では、情報の共有者の増減などによってACL8の設定を変

更する必要が生じると、その都度、企業外の運営者に対して設定作業を依頼する必要がある。したがって、それに要する手間や費用が大きな負担になるほか、外部の運営者を本当に信頼できるかといった信頼性の点においても問題が残ってしまう。

第6の実施形態の発明は上記の点に鑑みてなされたものであり、その目的は、チームデータリストが保存されているサーバの管理者にチームデータリストの管理を行わせずに、チームデータリストの管理者であるグループ内のメンバ自身がチームデータリストを管理でき、サーバ管理者、メンバではあるが管理者ではない者、クラッカなどがチームデータリストを不正に変更することを未然に防止できるチームデータリスト処理システムを提供することにある。また、本発明の別の目的は、チームデータリストの管理者として複数の者を設定できるようにして特定の個人にかかる作業負担を軽減することのできるチームデータリスト処理システムを提供することにある。さらに、本発明の他の目的は、サーバ管理者等の外部の者を介在することなくチームデータリストの管理者であるメンバ自身がチームデータリストの管理者の変更を行うことができるチームデータリスト処理システムを提供することにある。

以下、図面を参照して第6の実施形態について説明するが、まず初めに本発明におけるチームデータリストについて説明する。本発明におけるチームデータリストは、チームに関する情報を定義したリストの総称であって、上述したACLのような機密性の高い管理が要求される用途に適用される「メンバの集合」を定義するためのものである。上述した通り、従来のシステムでは、チームのメンバではない端末管理者、ネットワーク管理者、サーバ管理者などがチームに関する情報を変更することができる。一



方、本発明におけるチームデータリストでは、チームに関する情報を複数のリスト（後述するような１つ以上のメンバーリストとチームマスタリスト）に分割して管理することで、チームマスタ自身の変更といったチーム管理をチーム内のメンバだけで行えるようにしている。

次に、図６７ないし図６８を参照して本発明の前提となる技術について説明しておく。図６７は、本発明が前提とするシステムの構成をおおまかに描いたものであって、ネットワークNWとを介してクライアントCLととサーバSVとを接続して構成されたシステムである。図中、メンバーリストは各種の情報やユーザに提供される機能等の資源にアクセスできるメンバを記述したものである。また、サーバSVとはハードディスク上などに構築されたデータベース１０とに接続しており、このデータベース１０には複数のメンバが属するグループ（図中のグループAと、Bと）にそれぞれ対応したメンバーリスト１１Aと、１１Bとが記憶されている。

サーバSVとはメンバーリスト保管機能だけを備えており、クライアントCLとにメンバーリストを転送するほか、クライアントCLとが変更を行って返送してくるメンバーリストでデータベース１０上のメンバーリスト１１Aとやメンバーリスト１１Bとの内容を置き換える。その一方で、クライアントCLとはメンバーリスト管理機能を具備している。このメンバーリスト管理機能の一つにメンバーリストの変更機能があり、クライアントCLとはサーバSVとから取得したメンバーリストにメンバの追加や削除に応じた修正を行ってサーバSVとに返送するようにする。

ここで、いま説明した機能だけでは、サーバ管理者やクラッカなどがサーバSVとを操作することによって、クライアントCLと側のメンバーリス

ト管理機能を介在することなくサーバS Vと上のメンバリストを改竄できてしまう。しかも、サーバ管理者などが自らのデジタル署名で不正にメンバリストを改竄するとクライアントC Lとからは正当な管理者と区別できないという問題が生じる。この種の不都合を回避するために、図67のシステムではメンバリスト11Aと、11Bとにそれぞれデジタル署名12Aと、12Bとを付加している。また、これに対応するようにクライアントC Lとはメンバリスト管理機能の一環としてデジタル署名機能を備えており、秘密鍵ファイルや秘密鍵の記録されたIC（集積回路）カード等から秘密鍵を取得し、メンバリストに対してこの秘密鍵を用いたデジタル署名を施してサーバS Vとに送出するとともに、サーバS Vとがメンバリストとデジタル署名をグループ毎に対で保管するようにしている。こうすることで、メンバリストに付属するデジタル署名を確認することによって、サーバ管理者などがメンバリストの一部を不正に書き替えたことをクライアントC Lと側で見つけることができる。

一方、図68はクライアントC Lと側からサーバS Vと上のメンバリストを変更する場合の手順の概要を示したものである。サーバS Vと上に保管されているメンバリスト20とには、情報共有グループたるチームT1とを構成しているメンバMXと、MYと、…、MBと（実際は、次に述べるような各メンバに対応した公開鍵番号）に加えて、当該チームの管理者たるチームマスタTMと（詳細は後述）のデジタル署名が予め登録されている。

まず、メンバリストを変更する場合、クライアントC Lと側にいるチームマスタTMとは、グループないしチームを識別するためのグループID（識別子）と、公開鍵方式におけるユーザ公開鍵（即ち、所定長のビット

列) に対応したユーザ公開鍵番号 (図中のユーザ公開鍵 No) をサーバ S V とに送って、メンバリストを送るようにサーバ S V とへ要求する (ステップ S 1 と)。なお、ここで言う「ユーザ公開鍵番号」は、チームマスタ T M となどのユーザ本人を識別・認証するための情報であって、各ユーザ公開鍵に予め付与されているシリアル番号のことである。さらに詳しく説明すると、ユーザ公開鍵番号はユーザ公開鍵を一意に識別するための各ユーザ公開鍵に対応した情報であって、例えば、認証局から発行された証明書に含まれている当該証明書のシリアル番号である。また、ユーザ本人を識別・認証するための情報としては、いま述べたユーザ公開鍵番号以外にも、実際に鍵作成者本人を識別する I D や名前などの様々な情報を利用することができる。ちなみに、これ以後の説明ではこうしたユーザ本人を識別・認証するための情報の一例として公開鍵番号を用いた場合について説明を行う。

次に、サーバ S V とはクライアント C L とから送られてくるグループ I D、ユーザ公開鍵番号に基づいて以下に詳述するようにチームマスタ T M との権限を確認する (ステップ S 2 と)。まず、サーバ S V とは「シェイクハンド」又は「チャレンジレスポンス」と呼ばれる手法を用いてチームマスタ T M と本人の識別・認証を行う。以下、この処理について図 6 9 に示した手順に沿って説明する。まず、図 6 8 のステップ S 2 とのところで説明したように、クライアント C L とからサーバ S V とへのアクセスの際にユーザ名やユーザ公開鍵 (実際には上述したユーザ公開鍵番号) をサーバ S V と側に送付しておく (ステップ S 1 0 1 と)。次に、サーバ S V とは乱数を発生させて内部に記憶するとともにこの乱数を (ユーザ公開鍵番号に対応する) ユーザ公開鍵で暗号化 (ステップ S 1 0 2 と) し、暗号化されたデータを「チャレンジデータ」としてクライアント C L とに送信す

る（ステップS103と）。クライアントCLとはサーバSVとから送られたチャレンジデータをユーザ公開鍵に対応した秘密鍵で復号化（ステップS104と）し、得られた復号化データを「チャレンジレスポンス」としてサーバSVとに返送する（ステップS105と）。サーバSVとはクライアントCLとから送られたチャレンジレスポンスとステップS102とで発生させた乱数とを比較して通信相手を確認する。すなわち、両者が一致すればステップS101とで送付されたユーザ公開鍵に対応する秘密鍵を知っている者が通信相手であることを確認（認証成功）することができる。これに対し、両者が不一致であれば通信相手が正当な権限を持った者でない可能性のある（認証失敗）ことがわかる（以上、ステップS106と）。この後、サーバSVとはステップS106とで得られた確認結果（認証成功または認証失敗）をクライアントCLとに通知する（ステップS107と）。

このようにして仮に本人の認証が成功したならば、サーバSVとは、クライアントCLとから送られたユーザ公開鍵番号がメンバーリスト20とに記載されているかどうかを確認するとともに、ユーザ（この場合はチームマスタTMと）がメンバーリスト20とを変更する権限を持っているかどうかを確認する。ここでは、クライアントCLとから送られたユーザ公開鍵番号が、グループIDで指定されたチームT1とに対応するメンバーリスト20との中に記載されているものとする。ちなみに、ユーザ公開鍵番号がメンバーリスト20と上に記載されていなければ、サーバSVとは認証失敗をクライアントCLとに通知する。次に、サーバSVとは、メンバーリスト20と中のデジタル署名がチームマスタTMとのものであることから、サーバSVとはチームマスタTMとによるメンバーリストの書き換え要求を了承し、要求されたメンバーリスト20とをクライアントCLと側へ転送する（ステ

ップS 3 と)。クライアントCL とは、メンバリスト2 0 と内のデジタル署名を調べ、当該デジタル署名がチームマスタTM と自身の付与したものであることから、メンバリスト2 0 とがサーバSV と側で改竄されておらず正当なものであることを確認する（ステップS 4 と）。次に、クライアントCL とはメンバリスト2 0 と中のメンバMB とをメンバMC とに置き換えるメンバ変更処理を行ってメンバリスト2 1 とを作成する（ステップS 5 と）。ここで、作成されたメンバリスト2 1 とではメンバ変更の折りにデジタル署名を削除してあるので、クライアントCL とはメンバリスト2 1 とにチームマスタTM とのデジタル署名を付加したメンバリスト2 2 とを作成（ステップS 6 と）し、これをサーバSV とに返送する（ステップS 7 と）。

以上のようなことから、本発明ではメンバリストの管理自体はクライアントCL と側において各チーム内のメンバの中から選ばれた管理者が行うものとし、サーバSV と側では先に説明したサーバ管理者に相当する者やクラッカ等の無権限の者がメンバリストを不正に改竄できない構成を採用することにしている。そして、以下に詳述する本実施形態は、いま述べた前提技術を土台としてこれをさらに発展させたものであって、以下に述べる機能を盛り込むことで上述した本発明の目的を達成している。第一に、多数の人間を抱える部署のメンバリストを管理をするにあたって、一人の管理者にかかる負担を軽減するために、複数の管理者でメンバリストを管理する機構を実現する。第二に、チームデータリストの管理者自身によるチームデータリストの管理者の変更を実現する。例えば、チームデータリストの管理者である部長が異動になって後任の部長を新たなチームデータリストの管理者とする場合などである。そうした場合、チームデータリストの管理者たる現在の部長自身が管理者権限を後任の部長に権限委譲でき

るようにするほか、この権限委譲に際してサーバ管理者等の第三者が介入する余地のないようにしている。

そこで以下、チームデータリスト管理装置及びチームデータリスト保管装置の2つの装置を備えたシステムについて本実施形態を説明してゆく。図66は、チームデータリスト管理装置及びチームデータリスト保管装置を具備した本実施形態のシステム全体の構成を示したブロック図である。同図において、チームデータリスト管理装置30と、チームデータリスト保管装置31とは以下に詳述するチームデータリスト管理機能、チームデータリスト保管機能をそれぞれ備えており、互いに通信機能を利用してデータを授受している。チームデータリスト管理装置30と、チームデータリスト保管装置31とは何れもワークステーションなどの一般的なコンピュータで実現することが可能であり、これらコンピュータの主記憶上にはそれぞれチームデータリスト管理機能、チームデータリスト保管機能を実現するためのプログラム（チームデータリスト管理プログラム、チームデータリスト保管プログラム）が記憶される。

これらのプログラムはフロッピーディスク、IC（集積回路）カード、光磁気ディスク、CD-ROM（コンパクトディスクー読み取り専用メモリ）等の可搬性のある記憶媒体や、コンピュータに内蔵されるハードディスクなどの大容量の記憶媒体といったコンピュータ読み取り可能な記憶媒体にその一部又は全部が記憶されている。すなわち、当該プログラムは以下に詳述する機能の一部を実現するためのものであっても良く、さらにはコンピュータにすでに記録されているプログラムとの組み合わせでこれら機能を実現できるものであっても良い。そして、チームデータリスト管理装置やチームデータリスト保管装置を作動させ

るにあたって、これらのプログラムがコンピュータ上のCPU（中央処理装置）の指示の下に予め記憶媒体から主記憶上に転送される。その後、CPUは主記憶上に転送されたプログラムを実行し、それによって装置各部を制御して、以下に詳述する様々な処理を実現している。

本実施形態では、チームデータリストにアクセスできる者をその権限の内容に応じてメンバ、サブマスタ、チームマスタの3種類に分類しており、この順番でその者に付与される権限が拡大してゆく。サブマスタはチームマスタによって指名されたチーム内の管理者であって、チームマスタやサブマスタを変更することはできないが、一般のメンバに関して追加、削除といった変更を行うことのできる者である。一方、チームマスタはサブマスタ又はメンバの変更を行えるほか、自身のチームマスタでさえ変更することのできる者である。他方、サブマスタ及びチームマスタ以外の一般のメンバは情報や機能を共有する者であって、チームデータリストの内容に変更を加える等の権限はいっさい与えられていない。なお、サブマスタやチームマスタは特別な権限が与えられてはいるが、チーム内のメンバであることに変わりはなく、その意味でサブマスタ又はチームマスタをメンバと呼ぶことがある。

さて、図66に示すチームデータリスト保管装置31にはハードディスク等といったデータベースを構築可能な記憶装置32が接続されている。この記憶装置32は、複数のメンバで構成されるチーム毎にメンバリスト33とチームマスタリスト34とからなるチームデータリストの組を記憶している。同図では説明の都合からメンバリスト33及びチームマスタリスト34の組を一つだけ示しているが、実際にはチームの数だけこれらの組が存在している。メンバリスト33はユーザに提供され

る情報や機能を共有するメンバーの一覧で構成されており、メンバーの識別情報、メンバーに与えられた公開鍵、この公開鍵に対応する秘密鍵の所有者のID（以下「公開鍵ID」という）、チームを識別するチームID、リスト作成者（即ち、チームマスタ又はサブマスタ）のデジタル署名、当該メンバーリスト33とが作成された時間を示すタイムスタンプ、チーム内のメンバーが利用できる機能（例えば、アプリケーション）に関する情報、会社組織になぞらえてチームを階層化するための情報などが含まれている。このほか、メンバーリスト33とには各メンバーに関する情報として、e-mail（電子メール）アドレスやメンバー自身の住所といった情報も含まれており、これらを用いることで各メンバーに関する情報リソースの管理も同時に行うことができる。一方、チームマスタリスト34とはチームマスタ及びサブマスタの一覧で構成されており、チームマスタ又はサブマスタの識別情報、公開鍵、公開鍵ID、チームID、チームマスタのデジタル署名、当該チームマスタリスト34とが作成された時間を示すタイムスタンプなどが含まれる。このほか、チームマスタリスト34とには、チームに関する情報としてチームのメンバー数、チームの作成された時間、チーム内の各メンバーが利用することのできる各種機能などの情報も含まれており、これらを用いることで各チームに関する情報リソースの管理を同時に行うことができる。

次に、図66のチームデータリスト保管装置31とにおいて、権限確認機能35とはクライアントCLと側からメンバーリスト33とやチームマスタリスト34とに対する変更要求ないし参照要求があったときに、これら2つのリストの内容に基づき、クライアントCLと側の要求者自身の認証を行うほか、この要求者が変更ないし参照を行う正当な権限を有する者かどうか確認して、クライアントCLと側へメンバーリスト33とやチームマ



スタリスト 34 とを転送すべきかどうかを判断する。また、リスト保管機能 36 とは権限確認機能 35 とがメンバリスト 33 とやチームマスタリスト 34 とを使用するにあたって、これらのリストを記憶装置 32 とから取得しあるいは記憶装置 32 とへ保存する処理を司っている。以下の説明では、権限確認機能 35 とがメンバリスト 33 とやチームマスタリスト 34 とを使用する場合には必ずリスト保管機能 36 とが介在することを前提としているが、煩雑になるため一々説明しないことにする。

次に、チームデータリスト管理装置 30 とにおいて、リスト作成者確認機能 37 とはチームデータリスト保管装置 31 とからメンバリスト 33 と又はチームマスタリスト 34 とを取得し、それらリストが管理権限を持つ管理者（即ち、チームマスタ又はサブマスタ）によって作成されているかどうかを検証する。この検証によって、サーバ S V との管理者やサーバ S V とへ不正に侵入したクラッカ等の無権限の者がメンバリスト 33 とやチームマスタリスト 34 とを改竄したことを検知することができる。リスト変更機能 38 とは、リスト作成者確認機能 37 とが取得したメンバリスト 33 とやチームマスタリスト 34 とに対してメンバや管理者の追加、削除、置換などの変更を加えるものである。また、デジタル署名機能 39 とはリスト変更機能 38 とによって変更されたメンバリスト 33 とやチームマスタリスト 34 とに対し、変更者本人しか知り得ない秘密鍵ないしデジタル署名鍵を用いた暗号とハッシュ関数とを併用してこれらリストの変更者（即ち、チームマスタ又はサブマスタ）のデジタル署名を付加する。一方、公開鍵管理機能 40 とは、チームデータリスト管理装置 30 とに接続された公開鍵データベース 41 とにアクセスして、公開鍵と当該公開鍵に対応する公開鍵 ID を取得する。ちなみに、実際の形態においては、公開鍵データベース 41 とはチームデータリスト管理装置 30 とに直接的に接続さ

れたローカルな形態のみならず、インターネット等のネットワーク上に設置されたサーバ（例えば、認証局）に存在している形態も当然に考えられる。こうした形態によれば、公開鍵管理機能 40 とは例えば認証局上に登録されたホームページを介して公開鍵データベース 41 とにアクセスし、そこから上述した公開鍵及び公開鍵 ID をファイルの形式で取得することも可能になる。

なお、図 66 では公開鍵データベース 41 と、記憶装置 32 とをそれぞれチームデータリスト管理装置 30 と、チームデータリスト保管装置 31 ととは別構成としているが、例えば、チームデータリスト管理装置 30 とに公開鍵データベース 41 とを含めても良く、また、チームデータリスト保管装置 31 とに記憶装置 32 とを含めても良いのはもちろんである。

次に、上記構成によるチームデータリスト管理装置 30 とおよびチームデータリスト保管装置 31 とを有するシステムの動作について説明する。まず、図 70 は複数の管理者によってメンバを管理してゆく際の動作のうち、メンバリストに登録されているメンバの変更を行うための処理手順を示したものである。チームデータリスト保管装置 31 とにおいて、チームマスタリスト 45 とに対応するチーム T2 とは前述したチームマスタ TM とが作成したものであるため、チームマスタであるメンバ MX とのデジタル署名が付与されている。このチームマスタリスト 45 とでは、チームマスタとしてメンバ MX と、サブマスタとしてメンバ MY と及びメンバ MZ とが登録されている。なお以下の説明では、あるメンバがチームマスタ又はサブマスタである場合、それらメンバ（例えば図 70 に示したメンバ MX と、メンバ MY と）をそれぞれチームマスタ MX と、サブマスタ MY となどと表記することがある。

## 〔メンバーの変更〕

以下では、人事異動等でメンバーMBとがメンバーからはずれてメンバーMCとが新たなメンバーとして加入する場合を想定する。そのため、サブマスタMYとがチームT2とに属するメンバーMBとをメンバーMCとに置き換えるものとする。まず、チームデータリスト管理装置30とはチームT2とを表すグループIDおよびサブマスタMYとのユーザ公開鍵番号とともに、メンバーの変更要求をチームデータリスト保管装置31とに送出する（ステップS11と）。チームデータリスト保管装置31とにおいて、権限確認機能35とは上述したシェイクハンドによってサブマスタMYとの認証を行ったのち、グループIDで指定されるチームT2とに関わるメンバーリスト46とを参照してメンバーMYとのユーザ公開鍵番号が当該メンバーリスト46と上に存在することを確認するとともに、チームマスタリスト45とを参照することによって、サブマスタMYとがチームT2とのサブマスタであってメンバーの変更権限を有していることを確認する（ステップS12と）。次いで、権限確認機能35とは指定されたチームT2とに関するチームマスタリスト45と及びメンバーリスト46とをチームデータリスト管理装置30と側に転送する（ステップS13と）。

チームデータリスト管理装置30とにおいて、リスト作成者確認機能37とはチームデータリスト保管装置31とから転送されてきたチームマスタリスト45と及びメンバーリスト46とに含まれているデジタル署名を照合して、これらリストがチームマスタリスト45とに登録されている者（即ち、チームマスタMXと）によって作成された正当なものであることを確認する（ステップS14と）。

ここで、図 7 1 のフローチャートに基づいてリスト作成者確認機能 3 7 とが実施する確認処理の詳細について説明しておく。まず、リスト作成者確認機能 3 7 とはチームマスタリスト 4 5 と及びメンバリスト 4 6 とをチームデータリスト保管装置 3 1 とから取得（ステップ S 2 1 と）し、次いで、これら 2 つのリストに含まれるデジタル署名を確認する（ステップ S 2 2 と）。この確認の結果、何れか一つでもデジタル署名が改竄されているのであれば、不正行為が発生していると考えられるためいま行っているメンバ変更などの処理を中止する。一方、改竄が検出されなかったのであれば、リスト作成者確認機能 3 7 とはメンバリスト 4 6 とのデジタル署名者（即ち、図 7 0 ではメンバ MX と）がチームマスタリスト 4 5 とにチームマスタ又はサブマスタとして含まれていることを確認し、含まれていないのであれば不正行為があったものとしてステップ S 2 2 とにおけるのと同様に現在行っている処理を中止する（ステップ S 2 3 と）。

これに対して、メンバリスト 4 6 とのデジタル署名者がチームマスタリスト 4 5 とに含まれているのであれば、メンバリスト 4 6 との正当性については確認されたことになり、リスト作成者確認機能 3 7 とは引き続いてチームマスタリスト 4 5 とのデジタル署名者（即ち、図 7 0 では同じくメンバ MX と）がチームマスタであるかどうかを確認（ステップ S 2 4 と）し、チームマスタでなければステップ S 2 2 と～ステップ S 2 3 とと同様に、不正行為が発生したものとして処理を中止する。一方、チームマスタリスト 4 5 とのデジタル署名者がチームマスタであるならば、チームマスタリスト 4 5 とについても正当性が確認されたことになり、これ以後の処理を続行する。例えば上記の場合で言えば、リスト作成者確認機能 3 7 とがリスト変更機能 3 8 とに対してチームマスタリスト 4 5 と及びメンバリスト 4 6 とを送出する。

こうしてチームマスタリスト45と及びマスタリスト46との正当性が確認されたならば、図70のステップS15とにおいて、リスト変更機能38とはメンバリスト46とに記述されているメンバMBとをメンバMCとに置き換えてメンバリスト47とを作成し、これをデジタル署名機能39とに送出する。デジタル署名機能39とは前述した秘密鍵ファイル等からサブマスタMYとに関する秘密鍵を取得し、これを基にメンバリスト47とへサブマスタMYとのデジタル署名を添付したメンバリスト48とを作成（ステップS16と）したのち、チームマスタリスト45と及びメンバリスト48とをチームデータリスト保管装置31とに返送する（ステップS17と）。

チームデータリスト保管装置31とにおいて、権限確認機能35とは転送されてきたチームマスタリスト45と及びメンバリスト48とについてデジタル署名が改竄されていないかどうか検証するとともに、以下のようにしてこれらリストの内容を検証する。すなわち、チームマスタリスト45とのデジタル署名者はチームマスタMXとであることからその正当性が分かる。一方で、メンバリスト48とのデジタル署名者はサブマスタMYとであって、正当性の確認されたチームマスタリスト45とを参照することでこのサブマスタMYとがチームマスタMXとからメンバ変更を許可された者であることが分かるため、メンバリスト48とについてもそれが正当なものであることを信頼できる。これに対して、転送されてきたリストについて正当性が確認できない場合、権限確認機能35とはチームマスタリスト及びメンバリストを更新することなく処理を中止する（以上、ステップS18と）。以上のようにしてメンバリスト中のメンバ変更が行われたことになる。

## 〔サブマスタの変更〕

次に、チームマスタがサブマスタを変更する際の処理手順について図 7 2 を参照して説明する。以下では、チーム T 2 に属するチームマスタ MX とが、サブメンバたるメンバ MY とをメンバ MW とに置き換える場合を想定する。チームマスタ MX とがチームデータリスト管理装置 3 0 とに対してサブマスタをメンバ MY とからメンバ MW とへ変更する要求を行うと、チームデータリスト管理装置 3 0 とにおいてリスト作成者確認機能 3 7 とは図 7 0 のステップ S 1 1 とと同じくグループ ID 及びチームマスタ MX とのユーザ公開鍵番号とともにサブマスタの変更要求をチームデータリスト保管装置 3 1 とに送出する（ステップ S 3 1 と）。チームデータリスト保管装置 3 1 とにおいて、権限確認機能 3 5 とは図 7 0 のステップ S 1 2 とで説明したのと同様の手順に従って、シェイクハンドによりチームマスタ MX との認証を行ったのち、メンバ MX とのユーザ公開鍵番号がメンバリスト 4 6 とに記載されていることを確認するとともに、メンバ MX とがチーム T 2 とのチームマスタであってサブマスタの変更権限を与えられていることを確認する（ステップ S 3 2 と）。次に、権限確認機能 3 5 とは図 7 0 のステップ S 1 3 とと同様にしてチームマスタリスト 4 5 と及びメンバリスト 4 6 とをチームデータリスト管理装置 3 0 とに転送する（ステップ S 3 3 と）。

チームデータリスト管理装置 3 0 とにおいて、リスト作成者確認機能 3 7 とは転送されてきたチームマスタリスト 4 5 とに含まれているデジタル署名を調べる。これにより、リスト作成者確認機能 3 7 とはこのチームマスタリスト 4 5 とがチームマスタたるメンバ MX とによって作成された正当なものであることを確認し、チームマスタリスト 4 5 と及びメンバリス

ト46とをリスト変更機能38とに渡す（ステップS34と）。リスト変更機能38とはチームマスタリスト45とに記述されているサブマスタMYとをサブマスタMWとに置き換えたチームマスタリスト51とを作成し、これをデジタル署名機能39とに送出する（ステップS35と）。

デジタル署名機能39とは、前述した秘密鍵ファイル等からチームマスタMXとに関する秘密鍵を取得し、メンバーリスト51とに対してチームマスタMXとのデジタル署名を添付したチームマスタリスト52とを作成（ステップS36と）したのち、チームマスタリスト52と及びメンバーリスト46とをチームデータリスト保管装置31とに返送する（ステップS37と）。チームデータリスト保管装置31とにおいて、権限確認機能35とは転送されてきたチームマスタリスト52と及びメンバーリスト46との内容を図70のステップS18とと同様の手順に従って検証する。この場合、チームマスタリスト52と及びメンバーリスト46とのデジタル署名者は何れもチームマスタMXとであることからその正当性が分かる。これに対して、転送されてきたリストについて正当性が確認できない場合、権限確認機能35とはチームマスタリスト及びメンバーリストを更新することなく処理を中止する（ステップS38と）。以上のようにして、チームマスタリスト中のサブマスタの変更が行われたことになる。

なお、図72に示した事例では元々のメンバーリスト46とのデジタル署名がチームマスタMXとのものであったが、仮にこれがサブマスタMYとのデジタル署名であっても問題はない。すなわち、サブマスタの変更権限を有するチームマスタMXとは必ずメンバーリスト46とについて自身のデジタル署名を付与することができる。そこでこの場合は、チームデータリスト管理装置30側でメンバーリスト46とからサブマスタMYとのデジタ

ル署名を削除し、その代わりにチームマスタMXとのデジタル署名を添付してチームデータリスト保管装置31へと返送するようにする。こうすることで、メンバではなくなったサブマスタMYとのデジタル署名がなされたメンバリストがチームデータリスト保管装置31の側に残ることはなくなる。

〔チームマスタ自身の変更〕

次に、チームマスタがチームマスタ自身を変更する際の処理手順について図73に沿って説明する。以下では、チームマスタMXがチームマスタMKに権限委譲してチームマスタの交代を行う場合を想定している。チームデータリスト保管装置31に保管されているチームマスタリスト45とは図70又は図72に示したものと同一であって、メンバリスト48とは図70に示したメンバ変更後のものと同一である。

まず、チームマスタMXがチームデータリスト管理装置30に対してチームマスタをメンバMKに変更する要求を行うと、リスト作成者確認機能37とは、図70のステップS11と同様にして、グループID及びチームマスタMXのユーザ公開鍵番号とともにチームマスタリスト45及びメンバリスト48の参照要求をチームデータリスト保管装置31に送出する（ステップS41）。チームデータリスト保管装置31において、権限確認機能35とは図70のステップS12で説明したと同様の手順に従って、シェイクハンドによりメンバMXの認証を行ったのち、メンバMXのユーザ公開鍵番号がメンバリスト48に存在することを確認するとともに、メンバMXがチームT2のチームマスタであって要求しているリストの参照権限が与えられていることを確認する（ステップS42）。



次に、権限確認機能 35 とは図 70 のステップ S 13 とと同様にして指定されたチーム T 2 とに関するチームマスタリスト 45 と及びメンバリスト 48 とをチームデータリスト管理装置 30 とに転送する（ステップ S 43 と）。このとき、権限確認機能 35 とは後刻に行われる権限確認で使用するためにチームマスタリスト 45 とを保存しておく。次に、チームデータリスト管理装置 30 とにおいて、リスト作成者確認機能 37 とは転送されてきたチームマスタリスト 45 と、メンバリスト 48 とのデジタル署名をそれぞれ調べ、各々がチームマスタリスト 45 とに含まれるチームマスタ MX と、サブマスタ MY とによって作成された正当なものであることを確認する（ステップ S 44 と）。これにより、リスト作成者確認機能は転送された 2 つのリストをリスト変更機能 38 とに渡す。

次に、リスト変更機能 38 とはチームマスタリスト 45 と、メンバリスト 48 とに記述されているチームマスタたるメンバ MX とをメンバ MK とに置き換え、それぞれチームマスタリスト 55 と、メンバリスト 56 とを作成してこれらをデジタル署名機能 39 とに送出する（ステップ S 45 と）。デジタル署名機能 39 とは前述した秘密鍵ファイル等からチームマスタ MX とに関する秘密鍵を取得し、チームマスタリスト 55 と及びメンバリスト 56 とにそれぞれチームマスタ MX とのデジタル署名を添付したチームマスタリスト 57 と及びメンバリスト 58 とを作成してチームデータリスト保管装置 31 とに返送する（ステップ S 46 と）。

チームデータリスト保管装置 31 とにおいて、権限確認機能 35 とは転送されてきた 2 つのリストと先のステップ S 43 とで保存しておいたチームマスタリスト 45 と（即ち、旧チームマスタリスト）の 3 つのリストに

に基づき、図 7 4 に示すフローチャートに従って権限確認を行う（ステップ S 4 7 と）。また、図 7 5 はかかる権限確認を行う際に、図 7 4 の各ステップで比較照合されるチームマスタリストやメンバリストの様子を示したものである。

まず、権限確認機能 3 5 とは新旧のチームマスタリストとしてそれぞれチームマスタリスト 5 7 と、4 5 とを取得するとともに、新メンバリストとしてメンバリスト 5 8 とを取得する（ステップ S 6 1 と）。次に、権限確認機能 3 5 とはチームマスタリスト 5 7 と及びメンバリスト 5 8 とのデジタル署名をそれぞれ調べる（ステップ S 6 2 と）。もし何れかでも改竄されているのであれば、これら 2 つのリストがチームデータリスト管理装置 3 0 と（クライアント C L と）からチームデータリスト保管装置 3 1 と（サーバ S V と）へ転送される過程で不正行為が発生しているため、権限確認機能 3 5 とはチームマスタ変更処理を中止する。

一方、転送された 2 つのリストが何れも改竄されていなければ、権限確認機能 3 5 とは新チームマスタリスト 5 7 とのデジタル署名を調べて、それが旧チームマスタリスト 4 5 とのデジタル署名者と同じチームマスタ M X とによるものであることを確認する（ステップ S 6 3 と）。これは、元々チームマスタであった者から権限委譲が為されていることを確認するためであって、もしステップ S 6 3 との判断結果が“NO”となれば、権限違反などによる不正行為があると考えられるのでチームマスタ変更処理を中止する。

もつとも、この場合はチームマスタリスト 5 7 とにメンバ M X とのデジタル署名が添付されているので、権限確認機能 3 5 とは引き続いて、チー

ムマスタ自身の変更とこれ以外の通常の変更とを判別するために、新チームマスタリスト57とのデジタル署名者がマスタ権限を有しているかどうかを確認する（ステップS64）。例えば、前述した図70で説明したメンバ変更においてはチームマスタリスト45とのデジタル署名がマスタ権限を持つメンバMXによるものであり、このことは図72のサブマスタ変更におけるチームマスタ52についても同じである（即ち、ステップS64の判断結果が“YES”となる場合）。

一方、チームマスタ自身を変更する場合であるが、図73のステップS47の処理時点はメンバMXからメンバMKに権限委譲する移行期に相当しており、チームマスタリスト57は新管理者たるメンバMKがマスタであって且つ旧管理者たるメンバMXがデジタル署名した過渡的な状態になっており、チームマスタリスト57のデジタル署名者がマスタ権限を持っていないように見える。こうした状態が検出されてチームマスタ自身の変更を認識（ステップS64の判断結果が“NO”）したならば、権限確認機能35は新メンバリスト58のデジタル署名を調べ、そのデジタル署名が新チームマスタリスト57に含まれているか、さもなければ、新旧何れかのチームマスタリスト57、45のデジタル署名者であるかどうかを確認する（ステップS65）。もし、何れの条件も満足しないのであれば改竄等の不正行為が発生していると考えられるため、権限確認機能35はチームマスタ変更処理を中止する。もっとも、この場合はメンバリスト58のデジタル署名者が新旧チームマスタリスト57、45のデジタル署名者と同じであるため、権限確認機能35は正規の手続きを経てメンバリストが作成されたものと判断することができる。以上述べたステップS62～ステップS65の処理によって、正当な権限を持つチームマスタMXによる正常な操作でチームマ

スタ自身が変更されたものと判断することができる。

この後、権限確認機能 35 とは新旧チームマスタリスト 57 と、45 ととメンバリスト 58 とをチームデータリスト管理装置 30 とに送出する（ステップ S 48 と）。これ以後の処理は新たなチームマスタ MK との指示の下に行われるものであって、チームマスタリスト 57 ととメンバリスト 58 とのデジタル署名をチームマスタ MK とのデジタル署名で書き替えるための処理である。チームデータリスト管理装置 30 とにおいて、リスト作成者確認機能 57 とは転送されてきた各リストに含まれるデジタル署名を確認する（ステップ S 49 と）。すなわち、リスト作成者確認機能 37 とは旧チームマスタリスト 45 とと新メンバリスト 58 とのデジタル署名が何れも改竄されていないことを確認し、次いで新旧チームマスタリスト 57 と、45 とのデジタル署名が互いに一致しているかどうかを確認し、さらには旧チームマスタリスト 45 との内容をもとに当該リストのデジタル署名者たるメンバ MX とがチームマスタの権限を持っているかどうかを確認する。この場合は、いま述べた 3 つの条件を全て満足しているため、リスト作成者確認機能 37 とはチームマスタリスト 57 ととメンバリスト 58 とをリスト変更機能 38 とに渡す。

次に、リスト変更機能 38 とがチームマスタリスト 57 と及びメンバリスト 58 とを基にチームマスタリスト 59 と及びメンバリスト 60 とを作成してデジタル署名機能 39 とに渡す。デジタル署名機能 39 とは前述した秘密鍵ファイル等からメンバ MK とに関する秘密鍵を取得し、チームマスタリスト 59 と及びメンバリスト 60 との各々にメンバ MK とのデジタル署名を添付してチームマスタリスト 61 と及びメンバリスト 62 とを作成し、これらのリストをチームデータリスト保管装置 31 とに返送する（ス

テップS 5 0 と)。チームデータリスト保管装置 3 1 とにおいて、権限確認機能 3 5 とは転送されてきたチームマスタリスト 6 1 と及びメンバリスト 6 2 とに対して図 7 4 に示した処理手順に従って権限確認を行う（ステップS 5 1 と）。この場合は、これら 2 つのリストのデジタル署名者が何れもチームマスタMK とであるため、これら 2 つのリストが何れも正当なものであると判断することができる。なお、この場合は通常の変更であるため図 7 4 のステップS 6 4 とによる判断結果は“Y E S”となる。しかるに、もし転送されてきたリストについて正当性が確認できないのであれば、権限確認機能 3 5 とはチームマスタリスト及びメンバリストを更新することなく処理を中止する。以上によってチームマスタ自身の変更がなされたことになる。

なお、図 7 3 に示したステップS 4 7 とからステップS 5 1 とまでの移行期の間において、チームデータリスト管理装置 3 0 とからチームデータリスト保管装置 3 1 とに対してメンバリスト参照要求、メンバリスト変更要求、マスタ変更要求がなされた場合、チームデータリスト管理装置 3 0 と及びチームデータリスト保管装置 3 1 とでは以下のようにリスト作成者の確認が行われる。

まず、チームデータリスト管理装置 3 0 とからメンバリスト参照要求があると、チームデータリスト保管装置 3 1 とは旧チームマスタリスト 4 5 とと新メンバリスト 5 8 とをチームデータリスト管理装置 3 0 とに転送する。チームデータリスト管理装置 3 0 とにおいて、リスト作成者確認機能 3 7 とは転送されてきた 2 つのリストのデジタル署名が改竄されていないかどうかを確認したのち、旧チームマスタリスト 4 5 との内容をもとに当該リストのデジタル署名者（図 7 3 の場合はメンバMX と）がチームマス

タの権限を持っているかどうかを確認する。

一方、チームデータリスト管理装置 30 とからメンバリスト変更要求又はマスタ変更要求があると、チームデータリスト保管装置 31 とは新旧チームマスタリスト 57 と、45 と及び新メンバリスト 58 とをチームデータリスト管理装置 30 とへ転送する。チームデータリスト管理装置 30 とにおいて、リスト作成者確認機能 37 とはメンバリスト参照要求の場合と同様に、転送されてきた 2 つのリストのデジタル署名が改竄されていないかどうかを確認する。次に、リスト作成者確認機能 37 とは新旧チームマスタリスト 57 と、45 とのデジタル署名を互いに比較してこれらが一致しているかどうかを確認する。次いで、リスト作成者確認機能 37 とはメンバリスト参照要求の場合と同様に、旧チームマスタリスト 45 とのデジタル署名者がチームマスタの権限を持っているかどうかを確認する。

#### 〔チームマスタ確認の自動化〕

上述した実施形態では、チームデータリストを使用する都度、チームマスタが間違いなく本物であるかどうかをユーザがクライアント CL と側で確認する必要がある。例えば、チームデータリスト管理装置 30 とを構成するコンピュータのディスプレイ上に、“このリストは以下のメンバが管理者となって正常に管理されています。名前：メンバ MX と、組織：三菱マテリアル株式会社。作業を続行する場合は OK ボタンをマウスでクリックして下さい” などといったメッセージが表示される。このように、ユーザが当該メッセージを目視で確認する必要性が生じてくるため、ユーザに対して煩わしい印象を与える可能性がないとは言えない。こうした点を改善するには以下の機能をリスト作成者確認機能 37 とと連携する新たな機能として追加し、あるいは、リスト作成者確認機能 37 との一機能として組

み込むようにすることで解決される。

すなわち、チームマスタの公開鍵をチーム毎に予めクライアントCLと側の例えば公開鍵データベース41と（図66参照）に登録しておき、公開鍵管理機能40とが公開鍵データベース41とからチームマスタの公開鍵を取得してこれをリスト作成者確認機能37とに通知する。もしくは、公開鍵データベース41とには公開鍵に関する情報として公開鍵を識別するためのシリアル番号等を登録しておき、公開鍵管理機能40とがこのシリアル番号を公開鍵データベース41とから取得したのち、これをもとにチームデータリスト管理装置30との外部（例えばインターネット上）に登録されている公開鍵を別途取得してリスト作成者確認機能37とに渡すように構成しても良い。

一方、リスト作成者確認機能37とは、コンピュータのディスプレイ上に上述したようなメッセージを出す代わりに、公開鍵管理機能40とから通知されるチームマスタの公開鍵に基づいて、チームデータリスト保管装置31とから転送されてくるチームマスタリストに含まれているデジタル署名を確認するようにして、当該デジタル署名がチームマスタのものであるか判断する。こうすることで、ユーザがディスプレイ上の表示をもとに目視で確認することなくチームマスタの正当性を検証できるようになる。

#### 〔チームマスタ変更時におけるチームマスタ確認の自動化〕

ところで、図73に示したように正規の手続きでチームマスタが例えばメンバMXとからメンバMKとに変更された場合には、もはや旧管理者たるメンバMXとの公開鍵を使用することができなくなる。そのため、クライアントCLと側に登録されているチームマスタの公開鍵をユーザの介在

なしに自動的に変更してやる必要がある。かかる変更処理を実現するために、最終的なチームマスタリスト 61 と（図 73 参照）が作成されたのち（即ち、ステップ S51 との後）に以下の処理を行うことにすれば良い。

まず、チームデータリスト保管装置 31 とでは権限確認機能 35 とが旧チームマスタリスト、移行期のチームマスタリスト、最終的なチームマスタリスト（即ち、チームマスタリスト 45 と、57 と、61 と）をそれぞれチームデータリスト管理装置 30 とに転送する。チームデータリスト管理装置 30 とにおいて、リスト作成者確認機能 37 とは、公開鍵管理機能 40 とを通じて公開鍵データベース 41 とにおいてチームマスタとしてメンバMX とが登録されていることを知る。次に、リスト作成者確認機能 37 とはチームデータリスト保管装置 31 とから転送されてきた 3 つのリストから、旧管理者たるメンバMX とが正規の手続きに則って新管理者たるメンバMK とに権限委譲したことを確認することができる。

というのも、チームマスタリスト 45 と、57 と、61 とにそれぞれ登録されているチームマスタはメンバMX と→メンバMK と→メンバMK とと遷移しており、その一方で、これらリストに添付されているデジタル署名はそれぞれメンバMX と→メンバMX と→メンバMK とと遷移している。こうしたことから、リスト作成者確認機能 37 とは公開鍵管理機能 40 とを介在して公開鍵データベース 41 とにチームマスタとして登録されている者の公開鍵をメンバMX とのものからメンバMK とのものに変更する。なお、チームマスタの変更はそれほど煩雑に生じることはないことから、この変更処理を行うにあたってユーザに確認を求めるようにしても良い。また、チームマスタを確認するための情報としては公開鍵以外にも様々な情報を利用できるのはもちろんである。



なお、上述した実施形態では、メンバリストを一つだけ設けていたが、複数のメンバリストを用いるようにした場合であっても、チームマスタ自身の変更や複数のチームマスタによるリソース管理を実現することができる。例えば、各メンバの持つ権限に応じてメンバリストを2つ以上のメンバリストに細分化させることが考えられる。このようにすると、各メンバリストに属するメンバの共有する情報をメンバリストに応じて異なるものにすることが可能となる。

以上の通り、チームデータリスト管理プログラムを記録した記録媒体において

、チームデータリスト管理プログラムは、(1) 変更指示を行う指示者の本人識別・認証を行うための情報を所定の要求先に通知して、資源を互いに共有するメンバで構成されるチームに関わる情報と該情報の管理権限を有するマスタのデジタル署名とが含まれ、チームに属するメンバの権限に応じて用意されたチームデータリストを前記要求先から取得する処理と、

(2) 取得された該チームデータリストの内容に基づいて、権限を持つマスタが前記チームデータリストを作成したか否かを確認する確認処理と、

(3) 該確認処理によって権限を持つマスタの作成であることが確認された前記チームデータリストに対して前記変更指示に応じた変更を加えるリスト変更処理と、(4) 前記指示者のデジタル署名を作成し、前記リスト変更処理で変更されたチームデータリストに該デジタル署名を添付して前記要求先に送るデジタル署名処理とをコンピュータに実行させる。

また、上述のチームデータリスト管理プログラムは、前記メンバに関するメンバ情報及び前記マスタのデジタル署名が少なくとも含まれた1つ以上のメンバリストと、前記マスタの権限を示すマスタ情報及び前記マスタ

のデジタル署名が少なくとも含まれたマスタリストを前記チームデータリストとして用いている。

また、上述のチームデータリスト管理プログラムは、前記マスタには前記マスタリストの変更権限を有するチームマスタが含まれ、前記変更指示は前記チームマスタの変更指示であって、前記確認処理は、前記変更されたメンバリスト及びマスタリストを前記要求先に送出する処理と、該処理に対応して前記要求先から返送される移行期のメンバリスト及び移行期のマスタリストに含まれる前記マスタのデジタル署名を確認する処理とをさらに有し、前記デジタル署名処理は、前記変更指示で指定された変更後のチームマスタのデジタル署名を作成する処理と、前記移行期のメンバリスト及び移行期のマスタリストに該デジタル署名を付与した新メンバリスト及び新マスタリストを前記要求先に送り返す処理とをさらに有するものであっても良い。

また、上述のチームデータリスト管理プログラムは、前記チームマスタの本人識別を行うための識別情報を所定の場所から取得して予め登録しておく処理と、前記チームマスタの識別情報並びに前記要求先から送られてくる前記メンバリスト及び前記マスタリストに含まれる前記マスタのデジタル署名に基づいて、該マスタのデジタル署名が前記チームマスタのデジタル署名であるか否かを確認する処理とをさらにコンピュータに実行させるものであっても良い。

また、上述のチームデータリスト管理プログラムは、前記変更指示に際して取得したマスタリスト、前記移行期のマスタリスト及び前記新マスタリストの内容の変遷に基づいて、前記チームマスタが正規の手続きを経て変更されたことを確認する処理と、該変更が確認された場合に、前記変更指示で指定された変更後のチームマスタの識別情報を取得し、該識別情報により前記予め登録された変更前のチームマスタの識別情報を更新する処

理とをさらにコンピュータに実行させるものであっても良い。

一方、チームデータリスト保管プログラムを記録した記録媒体において、チームデータリスト保管プログラムは、(1) 資源を互いに共有するメンバーで構成されるチームに関わる情報と該情報の管理権限を有するマスタのデジタル署名が含まれ、チームに属するメンバーの権限に応じて用意されるチームデータリストを予め記憶しておく記憶処理と、(2) 所定の要求元から参照要求が送られた場合に、前記チームデータリスト及び該要求を行った指示者の本人識別・認証を行うための情報に基づいて前記指示者が前記要求の権限を有するか否かを判断して、前記指示者が前記要求の権限を有する場合にだけ前記要求元へ前記チームデータリストを送出する処理と、(3) 前記要求元から更新要求が送られた場合に、該要求元から送られてくるチームデータリストの内容に基づいて該チームデータリストの正当性を確認し、該正当性が確認された場合にのみ、記憶されている前記チームデータリストを更新する権限確認処理とをコンピュータに実行させる。

また、上述のチームデータリスト保管プログラムにおいて、前記記憶処理は、前記メンバーに関するメンバー情報と前記マスタのデジタル署名が少なくとも含まれた1つ以上のメンバーリストを予め記憶しておく処理と、前記マスタの権限を示すマスタ情報及び前記マスタのデジタル署名が少なくとも含まれたマスタリストを予め記憶しておく処理とをコンピュータに実行させるものであっても良い。

また、上述のチームデータリスト保管プログラムは、前記マスタには前記マスタリストの変更権限を有するチームマスタが含まれ、前記権限確認処理は、前記要求元から前記指示者による前記チームマスタの変更指示が通知された場合に、該変更前のマスタリストを旧マスタリストとして保存

する処理と、前記要求元からの要求によって前記マスタリスト及び前記メンバーリストを前記要求元に送出し、これらリストのうち、前記チームマスタに関する情報の変更された移行期のマスタリスト及び移行期のメンバーリストを前記要求元から受け取って前記チームマスタの変更を検出する処理と、該チームマスタの変更が検出された場合に、前記移行期のマスタリスト、前記移行期のメンバーリスト及び前記旧マスタリストに基づいて、前記チームマスタの変更の正当性を確認する処理と、該変更の正当性が確認された場合に、前記移行期のマスタリスト及び移行期のメンバーリストを前記要求元に送出し、これらリストに対して前記変更指示で指定された変更後のチームマスタのデジタル署名が添付された新マスタリスト及び新メンバーリストを前記要求元から受け取って正当性を確認し、該正当性が確認された場合にのみ記憶されている前記メンバーリスト及び記憶されている前記マスタリストを更新する処理とをさらにコンピュータに実行させるものであっても良い。

以上説明したように、第6の実施形態の発明には、以下のような効果がある。

本発明では、正当な権限を持つマスタからの変更指示に応じて、サーバ等に保管されているマスタリスト及びメンバーリスト等のチームデータリストを取得し、これらリストが権限を持つマスタによって正当に作成されたことを確認した後に、これらリストに変更を加えて要求先へ返すようにしている。こうしたことから、マスタ以外の一般のメンバ、サーバの管理者、クラッカ等の正当な権限を持たない者がチームデータリストを不正に操作したことを検知できる。

また、本発明では、チームマスタ自身がチームマスタの変更を行うことができるため、チームデータリストが保管されているサーバ等の管理者を

介在させることなくチームマスタの権限委譲を実現できる。しかも、複数の管理者でチームデータリストを管理してゆく仕組みを実現できるため、少数の管理者に負担が集中してしまうのを緩和させることが可能となる。

また、本発明では、チームデータリストに対してマスタのデジタル署名を含ませているため、チームデータリストに対してなされた改竄等の不正な行為を検出することが可能となる。

また、本発明では、チームデータリストの参照要求や更新要求がなされた場合に、これらの要求を行った指示者が権限を持つ者であるのかどうかの権限確認を実施するようにしているので、権限を持たない者による不正な行為を未然に防止することができる。

また、本発明では、公開鍵などのチームマスタ本人を識別・認証するための情報を予め登録しておき、チームデータリスト中のマスタのデジタル署名と照合するほか、チームマスタが変更された場合にはかかる変更を検出して、登録されているチームマスタの公開鍵等を適宜更新するようにしている。こうしたことから、チームデータリストを操作する度にユーザ自身がチームマスタを目視で確認するなどの煩わしい作業が必要なくなり、自動的にチームマスタの承認を行ってゆくことができる。

なお、ここでいう「コンピュータシステム」とは、OSや周辺機器等のハードウェアを含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フロッピーディスク、光磁気ディスク、ROM、CD-ROM等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの（伝送媒体、伝送波）、その場合のサーバやクライア

ントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであっても良い。

最後に、これらの実施の形態で必要な特徴のすべての組み合わせを列挙しているものではない。また、上記で説明した組み合わせ以外の組み合わせも発明になり得る。

## 請求の範囲

1. 共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能な情報共有システムであって、

少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能な情報保管装置と、

情報を見てもよい少なくとも一のメンバーの公開鍵を記憶する記憶部と、情報を暗号化するための共通鍵を用いる上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する暗号化部と、暗号化に用いた共通鍵を、上記記憶部に記憶され指定された公開鍵で暗号化し、暗号化鍵を生成する暗号化鍵生成部と、上記複数の暗号化鍵および暗号化データを上記情報保管装置に転送する転送部と、上記情報保管装置からメンバーリストを取得して、当該メンバーリストのチームマスターのデジタル署名が指定されたデジタル署名と一致するか否かを判断し、一致する場合にのみ追加するメンバーの公開鍵の登録または脱会するメンバーの公開鍵の削除を行い、追加登録または削除の場合、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含む新メンバーリストを作成して上記情報保管装置に転送するリスト管理部と、上記情報保管装置から所望の暗号化鍵情報および暗号化データを取得して、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で取得した暗号化データを復号する復号化部とを有する暗号化復号化装置と

を備えた情報共有システム。

2. 前記情報保管装置および前記暗号化複合化装置は、送信側から受信側へ情報またはデータが送信された場合、前記送信側から情報またはデ

一タの送信が行われたことを受信側に対し通知する送信通知と、受信側が確実に前記情報を受信したことを送信側に対し通知する受信通知とを行う送受信通知部を

さらに有する請求項 1 記載の情報共有システム。

3. 上記暗号化復号化装置は、上記情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得し、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成し、上記転送部に出力する出力部を

さらに有する請求項 1 記載の情報共有システム。

4. 共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、

グループに属するメンバーを追加登録または削除する場合、上記情報保管装置からメンバーリストを取得する工程と、

当該メンバーリストのチームマスターのデジタル署名が指定されたデジタル署名と一致するか否かを判断する工程と、

一致する場合にのみ、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含む新メンバーリストを作成する工程と、

作成したメンバーリストを上記情報保管装置に転送する工程と

を有する情報共有システムの情報処理方法。

5. 共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー



公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、

グループに属するメンバーで利用する共通鍵を登録する場合、上記情報保管装置からメンバーリストを取得する工程と、

当該メンバーリストのチームマスターのデジタル署名が指定されたデジタル署名と一致するか否かを判断する工程と、

一致する場合にのみ、上記指定されている公開鍵を用いて登録すべき共通鍵を暗号化する工程と、

暗号化された共通鍵を上記情報保管装置に転送する工程と

を有する情報共有システムの情報処理方法。

6. 共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、

送信側から受信側へ情報またはデータが送信された場合、前記送信側から情報またはデータの送信が行われたことを受信側に対し通知する送信通知と、受信側が確実に前記情報を受信したことを送信側に対し通知する受信通知を行う工程を

さらに有する請求項 5 記載の情報共有システムの情報処理方法。

7. 共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、お

よび暗号化データが保管されている情報共有システムの情報処理方法であって、

上記情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得する工程と、

この暗号化鍵情報から共通鍵を復号する工程と、

復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する工程と、

暗号化されたデータを上記情報保管装置に転送する工程と

を有する情報共有システムの情報処理方法。

8. 共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、

送信側から受信側へ情報またはデータが送信された場合、前記送信側から情報またはデータの送信が行われたことを受信側に対し通知する送信通知と、受信側が確実に前記情報を受信したことを送信側に対し通知する受信通知を行う工程を

さらに有する請求項7記載の情報共有システムの情報処理方法。

9. 共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、

上記情報保管装置から所望の暗号化鍵情報および暗号化データを取得する工程と、

この暗号化鍵情報から共通鍵を復号する工程と、

復号した共通鍵で取得した暗号化データを復号する工程と

を有する情報共有システムの情報処理方法。

10. 共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、

送信側から受信側へ情報またはデータが送信された場合、前記送信側から情報またはデータの送信が行われたことを受信側に対し通知する送信通知と、受信側が確実に前記情報を受信したことを送信側に対し通知する受信通知を行う工程を

さらに有する請求項9記載の情報共有システムの情報処理方法。

11. 少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置からメンバーリストを取得する工程と、

当該メンバーリストのチームマスターのデジタル署名が指定されたデジタル署名と一致するか否かを判断する工程と、

一致する場合にのみ、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含む新メンバーリストを作成する工程と、

作成したメンバーリストを上記情報保管装置に転送する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取

り可能な記録媒体。

1 2.        少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置からメンバーリストを取得する工程と、

      当該メンバーリストのチームマスターのデジタル署名が指定されたデジタル署名と一致するか否かを判断する工程と、

      一致する場合にのみ、上記指定されている公開鍵を用いて登録すべき共通鍵を暗号化する工程と、

      暗号化された共通鍵を上記情報保管装置に転送する工程と

      をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

1 3.        送信側から受信側へ情報またはデータが送信された場合、前記送信側から情報またはデータの送信が行われたことを受信側に対し通知する送信通知と、受信側が確実に前記情報を受信したことを送信側に対し通知する受信通知を行う工程を

      さらにコンピュータに実行させるプログラムを記録した請求項 1 2 に記載のコンピュータ読み取り可能な記録媒体。

1 4.        少なくとも複数のメンバーでアクセス可能で、少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得する工程と、

      この暗号化鍵情報から共通鍵を復号する工程と、

      復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する工程と、

暗号化されたデータを上記情報保管装置に転送する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

15. 送信側から受信側へ情報またはデータが送信された場合、前記送信側から情報またはデータの送信が行われたことを受信側に対し通知する送信通知と、受信側が確実に前記情報を受信したことを送信側に対し通知する受信通知を行う工程を

さらにコンピュータに実行させるプログラムを記録した請求項14に記載のコンピュータ読み取り可能な記録媒体。

16. 少なくともチームマスターのデジタル署名、メンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置から所望の暗号化鍵情報および暗号化データを取得する工程と、

この暗号化鍵情報から共通鍵を復号する工程と、

復号した共通鍵で取得した暗号化データを復号する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

17. 送信側から受信側へ情報またはデータが送信された場合、前記送信側から情報またはデータの送信が行われたことを受信側に対し通知する送信通知と、受信側が確実に前記情報を受信したことを送信側に対し通知する受信通知を行う工程を

さらにコンピュータに実行させるプログラムを記録した請求項16に記載のコンピュータ読み取り可能な記録媒体。

18. 少なくとも複数のメンバーでアクセス可能で、少なくともメンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能で、共通鍵暗号化方式および公開鍵暗号方

式を採用し、少なくともグループで共通鍵を共有可能なシステムに適用可能な情報保管装置であって、

メンバーリスト変更要求に応答して上記メンバーリストを変更可能なメンバーリスト管理部と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録し、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する共通鍵管理部と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管し、暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する暗号化データ管理部と

を有する情報保管装置。

19.       上記メンバーリスト管理部および共通鍵管理部は、特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記メンバーリストおよび共通鍵リストを変更する

請求項18記載の情報保管装置。

20.       上記メンバーリスト管理部および共通鍵管理部は、特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記メンバーリストおよび共通鍵リストを変更する

請求項18記載の情報保管装置。

21.       少なくとも複数のメンバーでアクセス可能で、少なくともメンバー公開鍵情報を含むメンバーリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能で、共通鍵暗号化方式および公開鍵暗号方

式を採用し、少なくともグループで共通鍵を共有可能なシステムに適用可能な情報保管装置の情報処理方法であって、

メンバーリスト変更要求に応答して上記メンバーリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と

を有する情報保管装置の情報処理方法。

22. 特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記メンバーリストおよび共通鍵リストを変更する工程

をさらに有する請求項21記載の情報保管装置の情報処理方法。

23. 特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記メンバーリストおよび共通鍵リストを変更する工程

をさらに有する請求項21記載の情報保管装置の情報処理方法。

24. メンバーリスト変更要求に応答して上記メンバーリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な

共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

25. メンバーリスト変更要求に応答して上記メンバーリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、

特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記メンバーリストおよび共通鍵リストを変更する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

26. メンバーリスト変更要求に応答して上記メンバーリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、



共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、

特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記メンバーリストおよび共通鍵リストを変更する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

27. メンバーリスト変更要求に応答して上記メンバーリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、

特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記メンバーリストおよび共通鍵リストを変更する工程と

特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記メンバーリ

ストおよび共通鍵リストを変更する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

28. 送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、

前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成部と、

前記受信内容確認情報を前記ネットワークを介して送信する送信部と、

前記ネットワークを介して前記受信内容確認情報を受信する受信部と、

前記送信者側端末から送信される前記情報と前記受信内容確認情報とを比較し

、この比較結果に基づいて改竄を検知する改竄検知部と

を具備する情報改竄検知装置。

29. 前記受信内容確認情報作成部は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか1つ、または複数組み合わせた情報に基づいて前記受信内容確認情報を作成する請求項28に記載の情報改竄検知装置。

30. 前記受信内容確認情報作成部は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか1つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づ

いて前記受信内容確認情報を作成する請求項 28 に記載の情報改竄検知装置。

31. 前記受信内容確認情報作成部は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか1つ、または複数組み合わせた情報に対してデジタル署名したものを前記受信内容確認情報として作成する請求項 28 に記載の情報改竄検知装置。

32. 前記受信内容確認情報作成部は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか1つ、または複数組み合わせた情報を作成し、

該組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェスト、および該組み合わせた情報に対してデジタル署名をしたものを作成し、

前記組み合わせた情報、前記メッセージダイジェスト、デジタル署名したもののうちいずれか2つ以上の情報を組み合わせたものを前記受信内容確認情報として作成する請求項 28 に記載の情報改竄検知装置。

33. 送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、

前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成部と、

前記受信内容確認情報を前記ネットワークを介して送信する送信部と、

前記ネットワークを介して前記受信内容確認情報を受信する受信部と、

前記送信者側端末から送信される前記情報と前記受信内容確認情報とを比較し

、この比較結果に基づいて改竄を検知する改竄検知部としてコンピュータを機能させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体。

34. 受信者側に設置された受信者側端末との間でネットワークを介して情報の送受信を行い、送信者側に設置された送信者側端末を有する情報改竄検知装置において、

前記送信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表し、かつ前記受信者側端末により生成された受信内容確認情報を前記ネットワークを介して受信する受信部と、

前記送信者側端末に設けられ、前記受信部により受信された前記受信内容確認情報と前記送信者側端末から送信される前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知部と

を具備する情報改竄検知装置。

35. 前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか1つ、または複数組み合わせた情報である請求項34に記載の情報改竄検知装置。

36. 前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか1つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストである請求項34に記載の情報改竄検知装置。

37. 前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか1つ、または複数組み合わせた情報に対してデジタル署名したものである請求項34に記載の情報改竄検知装置。

38. 前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか1つ、または複数組み合わせた情報に基づいて作成され、

該組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェスト、および該組み合わせた情報に対してデジタル署名をしたものに基づいて作成され、

前記組み合わせた情報、前記メッセージダイジェスト、デジタル署名したもののうちいずれか2つ以上の情報を組み合わせたものである請求項34に記載の情報改竄検知装置。

39. 受信者側に設置された受信者側端末との間でネットワークを介して情報の送受信を行い、送信者側に設置された送信者側端末を有する情報改竄検知装置において、

前記送信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表し、かつ前記受信者側端末により生成され、受信内容確認情報を前記ネットワークを介して受信する受信部と、

前記送信者側端末に設けられ、前記受信部により受信された前記受信内容確認情報と前記送信者側端末から送信される前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知部としてコンピュータを機能

させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体。

40. 送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、

前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成部と、

前記受信内容確認情報を前記ネットワークを介して送信する送信部と、

前記ネットワークを介して前記受信内容確認情報を受信する受信部と、

前記受信内容確認情報に基づいて、送信者側端末が、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を作成し、前記ネットワークを介して前記受信側端末へ送信する送信内容確認情報作成部と、

前記送信内容確認情報作成部から送信された前記送信内容確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知部と

を具備する情報改竄検知装置。

41. 前記送信内容確認情報作成部は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか1つ、または複数組み合わせた情報に基づいて前記送信内容確認情報を作成する請求項40に記載の情報改竄検知装置。

42. 前記送信内容確認情報作成部は、前記受信内容確認情報と前記確認情報のうちいずれか1つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて前記送信内容確認情報を作成する請求項40に記載の情報改竄検知装置。

43. 前記送信内容確認情報作成部は、前記受信内容確認情報と前記確

認情報のうちいずれか1つ、または複数組み合わせた情報に対してデジタル署名したものを前記送信内容確認情報として作成する請求項40に記載の情報改竄検知装置。

44. 前記送信内容確認情報作成部は、

前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか1つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストを前記送信内容確認情報として作成し、

前記受信内容確認情報と前記確認情報のうちいずれか1つ、または複数組み合わせた情報に対してデジタル署名したものを前記送信内容確認情報として作成し、

前記組み合わせた情報、前記メッセージダイジェスト、デジタル署名したもののうちいずれか2つ以上の情報を組み合わせたものに基づいて前記送信内容確認情報を作成する請求項40に記載の情報改竄検知装置。

45. 送信者側に設置された送信者側端末との間でネットワークを介して情報の送受信を行い、受信者側に設置された受信者側端末を有する情報改竄検知装置において、

前記受信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成部と、

前記受信者側端末に設けられ、前記受信内容確認情報を前記ネットワークを介して送信する送信部と、

前記受信者側端末に設けられ、前記受信内容確認情報に基づいて前記送信者側端末により作成される、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を前記ネットワークを介して受信し、該送信内容確認情報と、前記受信側端末により受信された前記情報とを比較し、

この比較結果に基づいて改竄を検知する改竄検知部と  
を具備する情報改竄検知装置。

46. 前記送信内容確認情報は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか1つ、または複数組み合わせた情報である請求項45に記載の情報改竄検知装置。

47. 前記送信内容確認情報は、前記受信内容確認情報と前記確認情報のうちいずれか1つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストである請求項45に記載の情報改竄検知装置。

48. 前記送信内容確認情報は、前記受信内容確認情報と前記確認情報のうちいずれか1つ、または複数組み合わせた情報に対してデジタル署名したものである請求項45に記載の情報改竄検知装置。

49. 前記送信内容確認情報は、

前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか1つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて作成され、

前記受信内容確認情報と前記確認情報のうちいずれか1つ、または複数組み合わせた情報に対してデジタル署名したものに基づいて作成され、

前記組み合わせた情報、前記メッセージダイジェスト、デジタル署名したもののうちいずれか2つ以上の情報を組み合わせたものである請求項45に記載の情報改竄検知装置。

50. 送信者側に設置された送信者側端末との間でネットワークを介して情報の送受信を行い、受信者側に設置された受信者側端末を有する情報改竄検知装置において、

前記受信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成部と、



前記受信者側端末に設けられ、前記受信内容確認情報を前記ネットワークを介して送信する送信部と、

前記受信者側端末に設けられ、前記受信内容確認情報に基づいて前記送信者側端末により作成される、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を前記ネットワークを介して受信し、該送信内容確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知部としてコンピュータを機能させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体。

5 1. 鍵暗号化部と、暗号化部とからなる暗号化装置において、

前記鍵暗号化部は、

共通鍵暗号方式を利用して暗号化に用いる共通鍵を取得または生成する共通鍵取得部と、

公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化鍵とする共通鍵暗号化部と、

前記共通鍵より共通鍵改竄検出に利用する鍵情報を作成する第1共通鍵改竄検出情報作成部とからなり、

前記暗号化部は、

前記共通鍵を用いて平文を暗号化し暗号文とするデータ暗号化部と、

前記平文より第1データ改竄検出情報を作成する第1データ改竄検出情報作成部とからなる暗号化装置。

5 2. 前記共通鍵暗号化部は、前記データ暗号化部により生成される暗号文を共有する利用者毎に、該利用者の公開鍵を用いて前記共通鍵を暗号化し暗号化鍵を生成する請求項5 1記載の暗号化装置。

5 3. 前記暗号化装置は、鍵復号化部をさらに備え、

前記鍵復号化部は、公開鍵暗号方式を利用して前記暗号化鍵を復号化す

る共通鍵復号化部と、

前記暗号化鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する第2共通鍵改竄検出情報作成部と、

前記鍵情報と前記共通鍵改竄検出情報を用いて改竄検証する第1改竄検証部とからなり、

前記鍵復号化部は、前記暗号化鍵を復号化し共通鍵を取得するとともに改竄検証し、

前記暗号化部は、前記共通鍵を用いて追加する平文をさらに暗号化する請求項51に記載の暗号化装置。

54. 請求項51に記載の暗号化装置によって暗号化された前記暗号化鍵と前記暗号文を復号化する、鍵復号化部と復号化部とからなる復号化装置において、

前記鍵復号化部は、公開鍵暗号方式を利用して前記暗号化鍵を復号化する共通鍵復号化部と、

前記暗号化鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する第2共通鍵改竄検出情報作成部と、

前記鍵情報と前記共通鍵改竄検出情報を用いて改竄検証する第1改竄検証部とからなり、

前記復号化部は、共通鍵暗号方式を利用して前記暗号文を復号化するデータ復号化部と、

前記暗号文を復号化した平文より第2データ改竄検出情報を作成する第2データ改竄検出情報作成部と、

前記第1データ改竄検出情報と前記第2データ改竄検出情報を用いて改竄検証する第2改竄検証部とからなる復号化装置。

55. 前記共通鍵復号化部は、暗号文を共有する利用者毎に対応する暗号化鍵のすべてを復号化し、

前記共通鍵改竄検出情報作成部は、復号化して得た共通鍵毎に前記共通鍵改竄検出情報を作成し、

前記第 1 改竄検証部は、前記鍵情報と前記共通鍵改竄検出情報から改竄検証を行なうとともに、利用者に対応する共通鍵を判定する請求項 5 4 に記載の復号化装置。

5 6. 請求項 5 1 に記載の暗号化装置と、請求項 5 4 に記載の復号化装置とから

構成される暗号化復号化装置。

5 7. 共通鍵暗号方式を利用し、暗号化に用いる共通鍵を取得または生成する手順と、

公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化鍵とする手順と、前記共通鍵より鍵情報を作成する手順と、

平文を共通鍵暗号方式を利用して暗号化し暗号文とする手順と、

前記平文より第 1 データ改竄検出情報を作成する手順とを具備する暗号化方法。

5 8. 公開鍵暗号方式を利用して前記暗号化鍵を復号化する手順と、

前記暗号化鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する手順と、

前記鍵情報と前記共通鍵改竄検出情報とから改竄検証する手順と、

前記暗号文を共通鍵暗号方式で復号化する手順と、

前記暗号文を復号化した平文より第 2 データ改竄検出情報を作成する手順と、前記第 1 データ改竄検出情報と前記第 2 データ改竄検出情報とから改竄検証する手順とを具備する復号化方法。

5 9. 共通鍵暗号方式を利用し、暗号化に用いる共通鍵を取得または生成する手順と、

公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化鍵とする手順と、

前記共通鍵より鍵情報を作成する手順と、

平文を共通鍵暗号方式を利用して暗号化し暗号文とする手順と、

前記平文より第1データ改竄検出情報を作成する手順とを

コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

60. 公開鍵暗号方式を利用して前記暗号化鍵を復号化する手順と、

前記暗号化鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する手順と、

前記鍵情報と前記共通鍵改竄検出情報とから改竄検証する手順と、

前記暗号文を共通鍵暗号方式で復号化する手順と、

前記暗号文を復号化した平文より第2データ改竄検出情報を作成する手順と、前記第1データ改竄検出情報と前記第2データ改竄検出情報とから改竄検証する手順とを

コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

61. チームを階層化するためのチームデータリストを管理するチームデータリスト管理装置であって、

所定の要求先に前記チームデータリストの操作要求を行い、該操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理者のデジタル署名を含むオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者のデジタル署名を含むオーソリティリストを有するチームデータリストを前記要求先から取得し、前記識別子を用いて取得されたチームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストのデジタル署名が改竄されていないこと及び前記管理

者情報を用いて権限を持つ者によるデジタル署名であることを確認して、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認部と、

該正当性確認部によって正当性が確認された前記チームデータリストに対して前記操作要求に応じた変更を加えるチームデータリスト変更部と、

前記操作要求を行った指示者のデジタル署名を作成し、前記変更されたチームデータリストに該デジタル署名を添付して前記要求先に送出するデジタル署名部と

を具備するチームデータリスト管理装置。

6 2. 前記管理者情報は、前記チームマスタにより自チーム内のメンバーから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報である請求項 6 1 記載のチームデータリスト管理装置。

6 3. 前記ルートチームのチームマスタの本人識別を行うための識別情報を所定の場所から取得して登録する登録部と、

予め登録されている前記識別情報を用いて、前記要求先から送られてくる前記ルートチームのオーソリティデータのデジタル署名が前記チームマスタのデジタル署名であることを確認するチームマスタ確認部とをさらに有する請求項 6 1 記載のチームデータリスト管理装置。

6 4. チームを階層化するためのチームデータリストを保管するチームデータリスト保管装置であって、

自チームの親チームを表す識別子及び前記親チームの管理者のデジタル署名が含まれたオーソリティデータをチーム毎に記憶するオーソリティデータ記憶部と、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チーム

の管理者のデジタル署名が含まれたオーソリティリストをチーム毎に記憶するオーソリティリスト記憶部と、

前記オーソリティデータ及び前記オーソリティリストが少なくとも含まれたチームデータリストに対する所定の要求元からの操作要求について、該操作要求の指示者が要求権限を持つことを前記管理者情報を用いて確認するとともに、参照要求或いは削除要求に対して要求されたチームデータリストを前記要求元へ返送し或いは削除し、更新要求に対しては、前記要求元から送られるチームデータリストのデジタル署名が権限を持つ者によるデジタル署名であることを前記管理者情報を用いて確認し、前記送られたチームデータリストで前記オーソリティデータ記憶部及び前記オーソリティリスト記憶部の記憶内容を更新する権限確認部と

を具備するチームデータリスト保管装置。

65. 前記管理者情報は、前記チームマスタにより自チーム内のメンバーから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報である請求項64記載のチームデータリスト保管装置。

66. 要求元である請求項61の何れかの項記載のチームデータリスト管理装置と、

要求先である請求項64記載のチームデータリスト保管装置とを有するチームデータリスト処理システム。

67. チームを階層化するためのチームデータリストを管理するチームデータリスト管理プログラムを記録した記録媒体であって、

所定の要求先に前記チームデータリストの操作要求を行う処理と、

前記操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理

者のデジタル署名が含まれたオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者のデジタル署名が含まれたオーソリティリストを有するチームデータリストを前記要求先から取得する処理と、

前記識別子を用いて取得された各チームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストのデジタル署名が改竄されていないこと及び前記管理者情報を用いて権限を持つ者によるデジタル署名であることを確認したのち、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認処理と、

該正当性確認処理によって正当性が確認された前記チームデータリストに対して前記操作要求に応じた変更を加える変更処理と、

前記操作要求を行った指示者のデジタル署名を作成して、前記変更処理によって変更されたチームデータリストに該デジタル署名を添付して前記要求先に送出する処理と

をコンピュータに実行させるためのチームデータリスト管理プログラムを記録した記録媒体。

68. チームを階層化するためのチームデータリストを保管するチームデータリスト保管プログラムを記録した記録媒体であって、

自チームの親チームを表す識別子及び前記親チームの管理者のデジタル署名が含まれたオーソリティデータをチーム毎に予め記憶しておく処理と、

自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者のデジタル署名が含まれたオーソリティリストをチーム毎に予め記憶しておく処理と、

所定の要求元から前記オーソリティデータ及び前記オーソリティリスト

が少なくとも含まれたチームデータリストに対する操作要求があったときに、該操作要求の指示者が要求権限を持つことを前記管理者情報を用いて確認するとともに、該操作要求が参照要求或いは削除要求である場合は、要求されたチームデータリストを前記要求元へ返送し或いは削除し、該操作要求が更新要求である場合は、前記要求元から送られるチームデータリストのデジタル署名が権限を持つ者によるデジタル署名であることを前記管理者情報を用いて確認したのち、前記送られたチームデータリストで記憶されている前記オーソリティデータ及び記憶されている前記オーソリティリストを更新する権限確認処理と

をコンピュータに実行させるためのチームデータリスト保管プログラムを記録した記録媒体。

69. 送信する情報を暗号化した暗号化情報を含む暗号情報を作成する暗号情報作成装置と、同報通信の被配信メンバーの公開鍵が含まれるメンバーリストを管理するメンバーリスト管理装置と、前記暗号化情報を復号化する暗号情報復号化装置と、前記暗号情報作成装置より送信された暗号情報を受信し、該暗号情報を前記メンバーリストをもとに1以上の前記暗号情報復号化装置に配信する情報中継装置と、からなる同報通信システムにおけるメンバーリスト管理装置であって、

同報通信を行う1以上のメンバーの公開鍵を含むメンバーリストを作成するリスト作成部と、

前記公開鍵を取得し保存する公開鍵管理部と  
を備えるメンバーリスト管理装置。

70. 前記メンバーリスト管理装置は、

ネットワークを介して端末から、もしくは、装置に接続された記憶媒体から、前記メンバーリストを取得し保存するリスト取得保存部をさらに備えた請求項69記載のメンバーリスト管理装置。



71. 前記メンバーリスト管理装置は、

前記メンバーリストをネットワークを介して、該ネットワークに接続されたデータベースまたは前記情報中継装置または前記メンバーリストに含まれるメンバーが利用する前記暗号情報作成装置ないし前記暗号情報復号化装置に送信するリスト送信部をさらに備えた請求項69に記載のメンバーリスト管理装置。

72. 前記メンバーリスト管理装置は、

同報通信のメンバーリストへの加入要求項目を設定する加入要求項目設定部と、

加入要求者により入力・転送された加入要求が、前記加入要求項目を満たし、メンバーリストへの加入を許可するか否かを判断する加入許可判断部と、

からなる加入要求受付部をさらに備える請求項69に記載のメンバーリスト管理装置。

73. 送信する情報を暗号化した暗号化情報を含む暗号情報を作成する暗号情報作成装置と、同報通信の被配信メンバーの公開鍵が含まれるメンバーリストを管理するメンバーリスト管理装置と、前記暗号化情報を復号化する暗号情報復号化装置と、前記暗号情報作成装置より送信された暗号情報を受信し、該暗号情報を前記メンバーリストをもとに1以上の前記暗号情報復号化装置に配信する情報中継装置と、からなる同報通信システムにおける暗号情報作成装置であって、

ネットワークを介して端末から、もしくは、装置に接続された記憶媒体から、前記メンバーリストを取得し保存するリスト取得保存部と、

同報通信文を取得し、該同報通信文を前記メンバーリストに含まれる公開鍵を用いて暗号化し暗号化情報とする暗号化部とを備えた暗号情報作成装置。

74. 前記暗号化部は、

前記同報通信文を共通鍵暗号方式で暗号化した暗号文を作成し、

前記共通鍵暗号方式で用いた共通鍵を、前記メンバーリストに含まれる1以上の公開鍵を用いて公開鍵暗号方式で暗号化した1以上の暗号化鍵を作成し、該暗号化鍵のうち、被配信メンバーに対応する暗号化鍵を選択するための鍵選択情報を作成し、

前記暗号情報として、前記暗号文、前記暗号化鍵、および前記鍵選択情報を出力する請求項73に記載の暗号情報作成装置。

75. 前記暗号化部は、

同報通信文が複数の構成要素で構成されている場合、前記暗号化部は前記同報通信文を構成する個々の構成要素毎に暗号化し前記暗号情報を作成する請求項73に記載の暗号情報作成装置。

76. 前記暗号情報作成装置は、

同報通信文の送信先を検査し該送信先が前記情報中継装置でありかつ前記リスト取得保存部からメンバーリストを取得できた場合、該同報通信文を前記暗号化部へ送る宛先検査部をさらに備えた請求項73に記載の暗号情報作成装置。

77. 前記暗号情報作成装置は、

同報通信文が主構成要素と1以上の従構成要素とからなる場合、主構成要素に対応する暗号情報に従構成要素に対応する暗号情報を参照可能とする参照情報を含め前記情報中継装置へ送信し、従構成要素に対応する暗号情報をネットワーク上の情報保管装置に送信する複数パーツ送信部をさらに備えた請求項73に記載の暗号情報作成装置。

78. 送信する情報を暗号化した暗号化情報を含む暗号情報を作成する暗号情報作成装置と、同報通信の被配信メンバーの公開鍵が含まれるメンバーリストを管理するメンバーリスト管理装置と、前記暗号化情報を復

号化する暗号情報復号化装置と、前記暗号情報作成装置より送信された暗号情報を受信し、該暗号情報を前記メンバーリストをもとに1以上の前記暗号情報復号化装置に配信する情報中継装置と、からなる同報通信システムにおける暗号情報復号化装置であって、

前記情報中継装置から転送された暗号情報を取得する暗号情報取得部と、

前記暗号情報に含まれる暗号化情報を復号化する復号化部とを備えた暗号情報復号化装置。

79. 前記復号化部は、

前記暗号情報に含まれる鍵選択情報を参照し復号化に利用する暗号化鍵を選択する鍵選択部と、

公開鍵暗号方式を利用して前記選択した暗号化鍵を受信者の秘密鍵で復号化し、共通鍵を得る暗号化鍵復号化部と、

共通鍵暗号方式を利用して、前記共通鍵を用いて前記暗号情報に含まれる暗号化情報を復号化し、平文の同報通信文を得る暗号文復号化部とからなる請求項78に記載の暗号情報復号化装置。

80. 前記暗号情報復号化装置は、

被配信メンバー本人が受信したことを通知する受信通知を前記情報中継装置に発信する受信通知発信部をさらに備える請求項78に記載の暗号情報復号化装置。

81. 前記暗号情報復号化装置は、

同報通信文が主構成要素と1以上の従構成要素とからなる場合、従構成要素に対応する暗号情報を参照可能とする参照情報を含む主構成要素に対応する暗号情報を受信し、前記参照情報をもとに従構成要素に対応する暗号情報を受信する複数パーツ受信部をさらに備える請求項78に記載の暗号情報復号化装置。

82. 前記暗号情報復号化装置は、

前記暗号情報作成装置における暗号情報作成時に用いられたメンバーリストと、前記配信先リストを作成するために利用したメンバーリストの同一性の検証、暗号情報の送信者がメンバーリストに含まれた者であるかどうかの検証、通信経路上で暗号情報が改竄されていないか検証する完全性の検証、

転送されてきた情報の中に悪意あるプログラムやデータ列が含まれているかどうかの検証、

転送されてきた暗号情報を参照して暗号情報作成装置で作成された複数のパーツからなる暗号情報のうち、一部が別の情報保管装置に転送されているかどうかの検証、

のいずれかもしくはは組合わせによる前記検証を行なう同報通信安全性検証部をさらに備える請求項 7 8 に記載の暗号情報復号化装置。

8 3. 前記暗号情報復号化装置は、

ネットワークを介してメンバーリストを既に保存している装置から、前記メンバーリストを取得し保存するリスト取得保存部をさらに備えた請求項 7 8 に記載の暗号情報復号化装置。

8 4. 送信する情報を暗号化した暗号化情報を含む暗号情報を作成する暗号情報作成装置と、同報通信の被配信メンバーの公開鍵が含まれるメンバーリストを管理するメンバーリスト管理装置と、前記暗号化情報を復号化する暗号情報復号化装置と、前記暗号情報作成装置より送信された暗号情報を受信し、該暗号情報を前記メンバーリストをもとに 1 以上の前記暗号情報復号化装置に配信する情報中継装置と、からなる同報通信システムにおける情報中継装置であって、

配信先リストを管理する配信先リスト管理部と、

転送されてきた暗号情報を複製する情報複製部と、

複製された暗号情報を各被配信メンバーに配信する送信部とを備える情

報中継装置。

85. 前記配信先リスト管理部は、

必要なときに保存先からメンバーリストを取得可能であり、転送されたメンバーリストを保存するリスト取得保存部と、

チームマスターから転送されてきたメンバーリストに含まれるメンバーと同じメンバーに情報が配信されるように配信先リストを変更する請求項84に記載の情報中継装置。

86. 前記情報中継装置は、

メンバーリストに添付されたデジタル署名の正当性を確認する際に、該対応テーブルを参照して、自動的に正当なチームマスター本人のデジタル署名かどうかを判断させるリスト正当性確認部をさらに備える請求項84に記載の情報中継装置。

87. 前記情報中継装置は、

転送されてきた情報の全部または一部に添付情報を添付する付加情報添付部をさらに備える請求項84に記載の情報中継装置。

88. 前記情報中継装置は、

前記暗号情報作成装置における暗号情報作成時に用いられたメンバーリストと、前記配信先リストを作成するために利用したメンバーリストの同一性の検証、 情報受信を拒否する受信側端末または利用者の識別情報が含まれる受信拒否情報を取得し、情報中継装置に転送されてきた情報の送信者または送信側端末が、前記受信拒否情報に含まれているか否かの検証、

暗号情報の送信者がメンバーリストに含まれた者であるかかどうかの検証、

通信経路上で暗号情報が改竄されていないか検証する完全性の検証、

転送されてきた情報の中に悪意あるプログラムやデータ列が含まれているかどうかの検証、

転送されてきた暗号情報を参照して暗号情報作成装置で作成された複数のパーツからなる暗号情報のうち、一部が別の情報保管装置に転送されているかどうかの検証、

のいずれかもしくはは組合わせによる前記検証を行なう同報通信安全性検証部をさらに備える請求項 8 4 に記載の情報中継装置。

8 9. 前記情報中継装置は、

転送されてきた情報、または、情報の一部を保存しておく同報通信内容保存部をさらに備える請求項 8 4 に記載の情報中継装置。

9 0. 前記情報中継装置は、

同報通信サービスの開設受付の際に開設要求者が満たすべき開設要求項目を開設要求者の端末に提示させる開設要求項目提示部と、

前記開設要求者が転送した開設受付要求が、前記開設要求項目を満たし、同報通信サービスの開設を許可するか否かを判断する開設許可判断部と、

前記開設許可判断部により同報通信サービスの開設が決定されると、前記開設要求者をチームマスターとし、該チームマスターが指定したメンバーに情報を配信する同報通信サービスを開設する同報通信開設部と、

を含む同報通信自動開設部をさらに備える請求項 8 4 に記載の情報中継装置。

9 1. 請求項 6 9 に記載のメンバーリスト管理装置と、請求項 7 3 に記載の暗号情報作成装置と、請求項 7 8 に記載の暗号情報復号化装置と、請求項 8 4 に記載の情報中継装置とからなる同報通信システム。

9 2. 前記メンバーリスト管理装置におけるメンバーリスト管理プログラムを記録した記録媒体であって、

同報通信を行う 1 以上のメンバーの公開鍵を含むメンバーリストを作成する手順と、

前記公開鍵を取得し保存する手順とを

をコンピュータに実行させるメンバーリスト管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

93. 前記暗号情報作成装置における暗号情報作成プログラムを記録した記録媒体であって、

ネットワークを介して、メンバーリストを取得し保存する手順と、

同報通信文を取得し、該同報通信文を前記メンバーリストに含まれる公開鍵を用いて暗号化し暗号化情報とする手順と

をコンピュータに実行させる暗号情報作成プログラムを記録したコンピュータ読み取り可能な記録媒体。

94. 前記暗号情報復号化装置における暗号情報復号化プログラムを記録した記録媒体であって、

前記情報中継装置から転送された暗号情報を取得する手順と、

前記暗号情報に含まれる暗号化情報を復号化する手順と

をコンピュータに実行させる暗号情報復号化プログラムを記録したコンピュータ読み取り可能な記録媒体。

95. 前記情報中継装置における情報中継プログラムを記録した記録媒体であって、

配信先リストを管理する手順と、

転送されてきた暗号情報を複製する手順と、

複製された暗号情報を各被配信メンバーに配信する手順と

をコンピュータに実行させる情報中継プログラムを記録したコンピュータ読み取り可能な記録媒体。

96. 変更指示を行う指示者の本人識別・認証を行うための情報を所定の要求先に通知して、資源を互いに共有するメンバで構成されるチームに関わる情報と該情報の管理権限を有するマスタのデジタル署名とが含まれ、チームに属するメンバの権限に応じて用意されたチームデータリスト

を前記要求先から取得し、取得された該チームデータリストの内容に基づいて、権限を持つマスタが前記チームデータリストを作成したか否かを確認するリスト作成者確認部と、

該権限を持つマスタの作成であることが確認された前記チームデータリストに対して前記変更指示に応じた変更を加えるリスト変更部と、

前記指示者のデジタル署名を作成し、前記リスト変更部で変更されたチームデータリストに該デジタル署名を添付して前記要求先に送るデジタル署名部と

を具備するチームデータリスト管理装置。

97. 前記チームデータリストには、前記メンバに関するメンバ情報及び前記マスタのデジタル署名が少なくとも含まれた1つ以上のメンバリストと、前記マスタの権限を示すマスタ情報及び前記マスタのデジタル署名が少なくとも含まれたマスタリストが含まれている請求項96記載のチームデータリスト管理装置。

98. 前記マスタには前記マスタリストの変更権限を有するチームマスタが含まれ、前記変更指示は前記チームマスタの変更指示であって、

前記リスト作成者確認部は、前記要求先に送られた前記変更されたメンバリスト及びマスタリストに対応して前記要求先から返送される移行期のメンバリスト及び移行期のマスタリストに含まれる前記マスタのデジタル署名を確認し、

前記デジタル署名部は、前記変更指示で指定された変更後のチームマスタのデジタル署名を作成し、前記移行期のメンバリスト及び移行期のマスタリストに該デジタル署名を付与した新メンバリスト及び新マスタリストを前記要求先に送り返す請求項97記載のチームデータリスト管理装置。

99. 前記チームマスタの本人識別を行うための識別情報を所定の場所から取得して登録する登録部と、



前記チームマスタの識別情報並びに前記要求先から送られてくる前記メンバーリスト及び前記マスタリストに含まれる前記マスタのデジタル署名に基づいて、該マスタのデジタル署名が前記チームマスタのデジタル署名であるか否かを確認するチームマスタ確認部とをさらに有する請求項 98 記載のチームデータリスト管理装置。

100. 前記変更指示に際して取得したマスタリスト、前記移行期のマスタリスト及び前記新マスタリストの内容の変遷に基づいて、前記チームマスタが正規の手続きを経て変更されたことを確認する変更確認部と、

該変更が確認されたことを条件として、前記変更指示で指定された変更後のチームマスタの識別情報を取得し、該識別情報により前記登録部に登録されている変更前のチームマスタの識別情報を更新する識別情報更新部とをさらに有する請求項 99 記載のチームデータリスト管理装置。

101. 資源を互いに共有するメンバで構成されるチームに関わる情報と該情報の管理権限を有するマスタのデジタル署名とが含まれ、チームに属するメンバの権限に応じて用意されるチームデータリストを記憶するチームデータリスト記憶部と、

所定の要求元からの参照要求に対し、前記チームデータリスト及び該要求を行った指示者の本人識別・認証を行うための情報に基づいて前記指示者が前記要求の権限を有するか否かを判断し、権限を有する指示者の居る要求元に対してだけ前記チームデータリストを送出する第 1 の権限確認部と、

前記要求元からの更新要求に対し、該要求元から送られてくるチームデータリストの内容に基づいて該チームデータリストの正当性を確認し、正当性の確認されたチームデータリストで前記チームデータリスト記憶部の記憶内容を更新する第 2 の権限確認部と

を具備するチームデータリスト保管装置。

102. 前記チームデータリスト記憶部は、

前記メンバに関するメンバ情報と前記マスタのデジタル署名が少なくとも含まれた1つ以上のメンバリストを記憶するメンバリスト記憶部と、

前記マスタの権限を示すマスタ情報及び前記マスタのデジタル署名が少なくとも含まれたマスタリストを記憶するマスタリスト記憶部と

を有する請求項101記載のチームデータリスト保管装置。

103. 前記マスタには前記マスタリストの変更権限を有するチームマスタが含まれ、前記第2の権限確認部は、

前記指示者から通知される前記チームマスタの変更指示に対し、該変更前のマスタリストを旧マスタリストとして保持するマスタリスト保持部と、

前記要求元からの要求で前記要求元に送出した前記マスタリスト及び前記メンバリストのうち、前記チームマスタに関する情報の変更された移行期のマスタリスト及び移行期のメンバリストを前記要求元から受け取り、これらリストに基づいて前記チームマスタの変更を検出する部と、

該変更が検出されたことを条件として、前記移行期のマスタリスト、前記移行期のメンバリスト及び前記旧マスタリストに基づいて、前記チームマスタの変更の正当性を確認する部と、

該正当性が確認されたことを条件として前記要求元に送出された前記移行期のマスタリスト及び移行期のメンバリストに対し、前記変更指示で指定された変更後のチームマスタのデジタル署名が添付された新マスタリスト及び新メンバリストを前記要求元から受け取り、これらリストの正当性を確認して前記メンバリスト記憶部及び前記マスタリスト記憶部の記憶内容を更新する部と

をさらに有する請求項102記載のチームデータリスト保管装置。

104. 要求元である請求項96に記載のチームデータリスト管理装置と、

要求先である請求項 1 0 1 に記載のチームデータリスト保管装置とを有するチームデータリスト処理システム。

1 0 5. 変更指示を行う指示者の本人識別・認証を行うための情報を所定の要求先に通知して、資源を互いに共有するメンバで構成されるチームに関わる情報と該情報の管理権限を有するマスタのデジタル署名とが含まれ、チームに属するメンバの権限に応じて用意されたチームデータリストを前記要求先から取得する処理と、

取得された該チームデータリストの内容に基づいて、権限を持つマスタが前記チームデータリストを作成したか否かを確認する確認処理と、

該確認処理によって権限を持つマスタの作成であることが確認された前記チームデータリストに対して前記変更指示に応じた変更を加えるリスト変更処理と、 前記指示者のデジタル署名を作成し、前記リスト変更処理で変更されたチームデータリストに該デジタル署名を添付して前記要求先に送るデジタル署名処理と

をコンピュータに実行させるためのチームデータリスト管理プログラムを記録した記録媒体。

1 0 6. 資源を互いに共有するメンバで構成されるチームに関わる情報と該情報の管理権限を有するマスタのデジタル署名が含まれ、チームに属するメンバの権限に応じて用意されるチームデータリストを予め記憶しておく処理と、 所定の要求元から参照要求が送られた場合に、前記チームデータリスト及び該要求を行った指示者の本人識別・認証を行うための情報に基づいて前記指示者が前記要求の権限を有するか否かを判断して、前記指示者が前記要求の権限を有する場合にだけ前記要求元へ前記チームデータリストを送出する処理と、

前記要求元から更新要求が送られた場合に、該要求元から送られてくるチームデータリストの内容に基づいて該チームデータリストの正当性を確

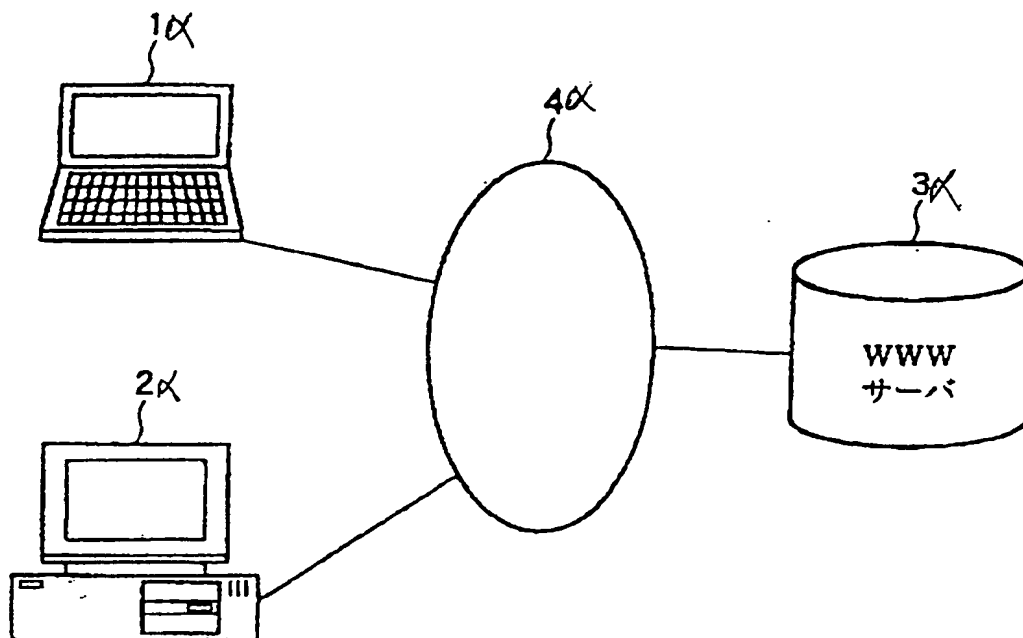
認し、該正当性が確認された場合にのみ、記憶されている前記チームデータリストを更新する権限確認処理と

をコンピュータに実行させるためのチームデータリスト保管プログラムを記録した記録媒体。

*This Page Blank (uspto)*

1/7 3

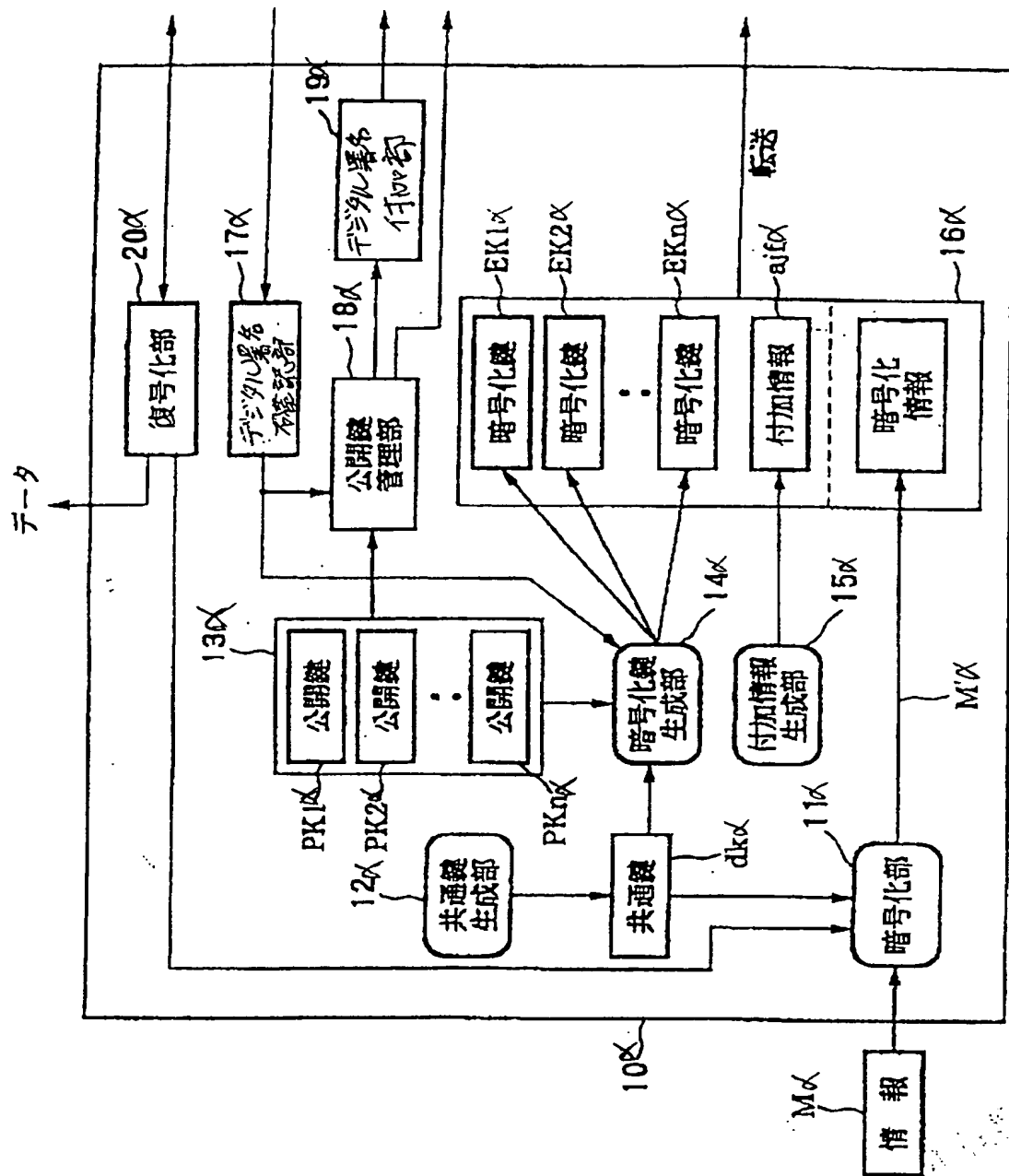
図 1



*This Page Blank (usph)*

2/7 3

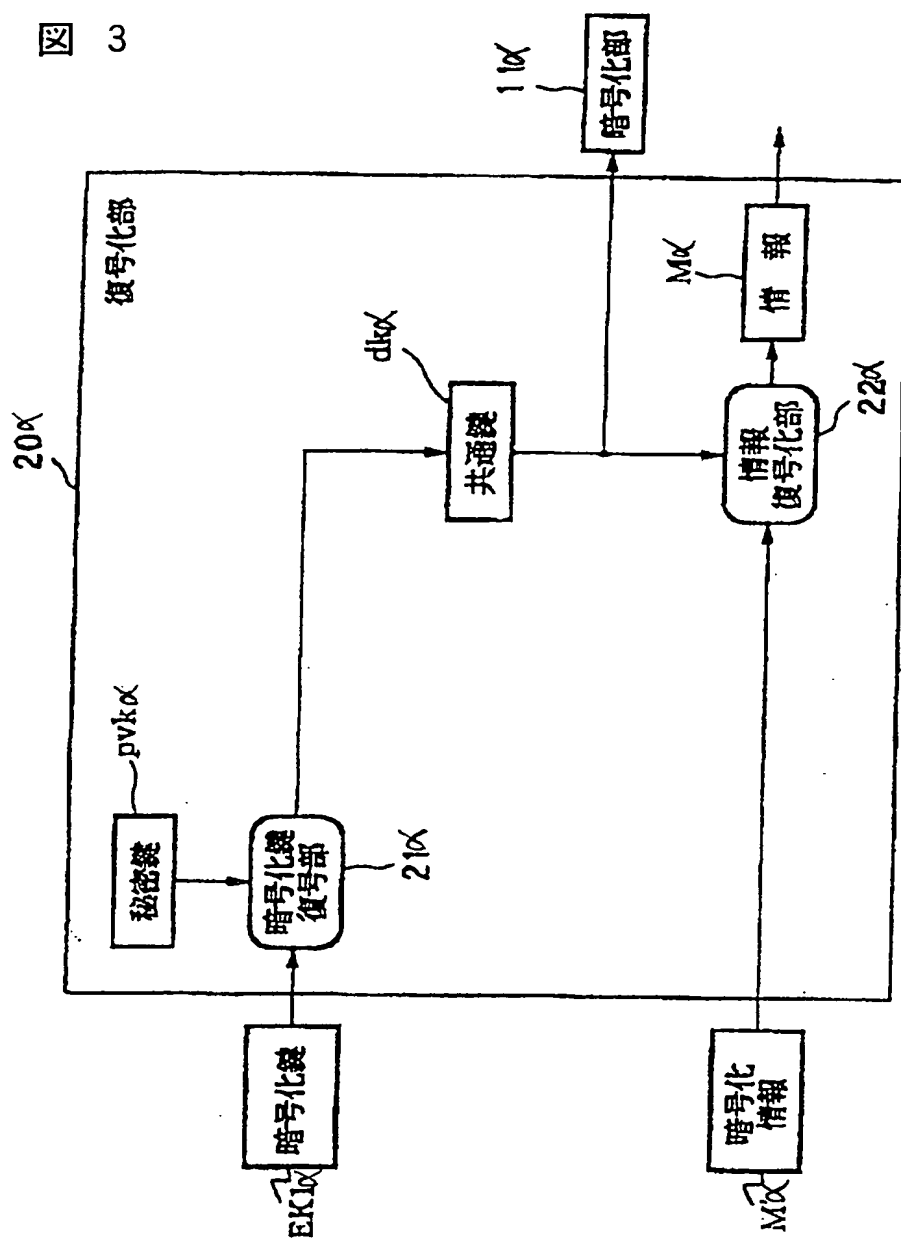
図 2



*This Page Blank (uspto)*



図 3



*This Page Blank (uspro)*

4/7 3

図 4

31X

32X

DBMS

権限確認部

X=バーリスト GLX

| グループID | 公開鍵No | メンバー公開鍵 | チームマスター<br>デジタ署名 |
|--------|-------|---------|------------------|
| :      | :     | :       |                  |

共通鍵リスト CKLX

| 共通鍵No | 公開鍵No | 暗号化鍵 |
|-------|-------|------|
| 122   | 11:AA | qwer |
| 122   | 1C:FF | zxcv |
| 122   | E5:4B | wert |

グループの共通鍵リスト GCKLX

| グループID | 共通鍵No |
|--------|-------|
| Bチーム   | 123   |

暗号化データリスト EDLX

| データID | 暗号化データ    |
|-------|-----------|
| 4444  | iiiiiiiii |

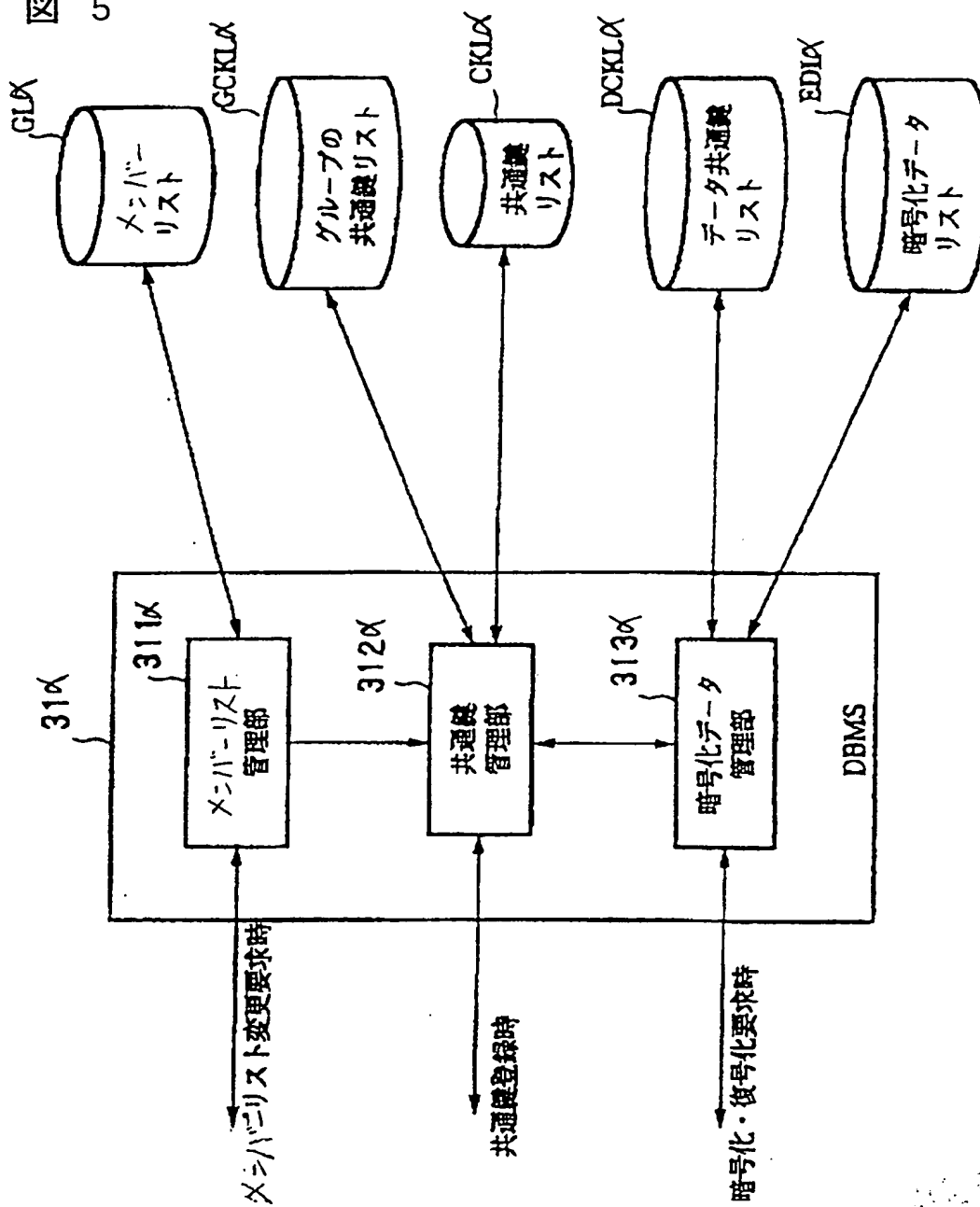
データ共通鍵リスト DCKLX

| データID | 共通鍵No |
|-------|-------|
| 4444  | 123   |

*This Page Blank (uspto)*

5/7 3

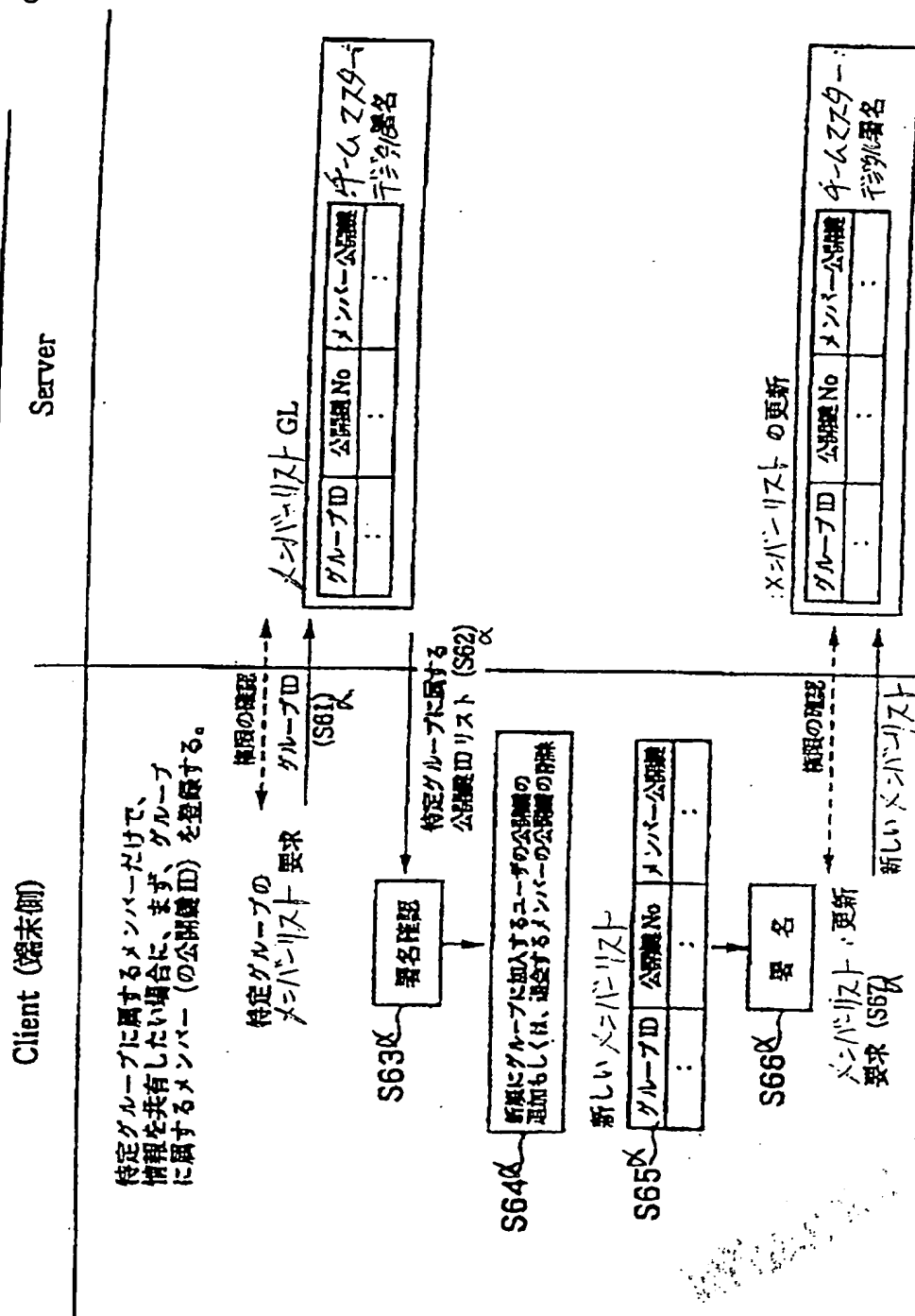
図 5



*This Page Blank (uspto)*

図 6

グループへの公開鍵ID登録例（グループで共通鍵を共有する方式）



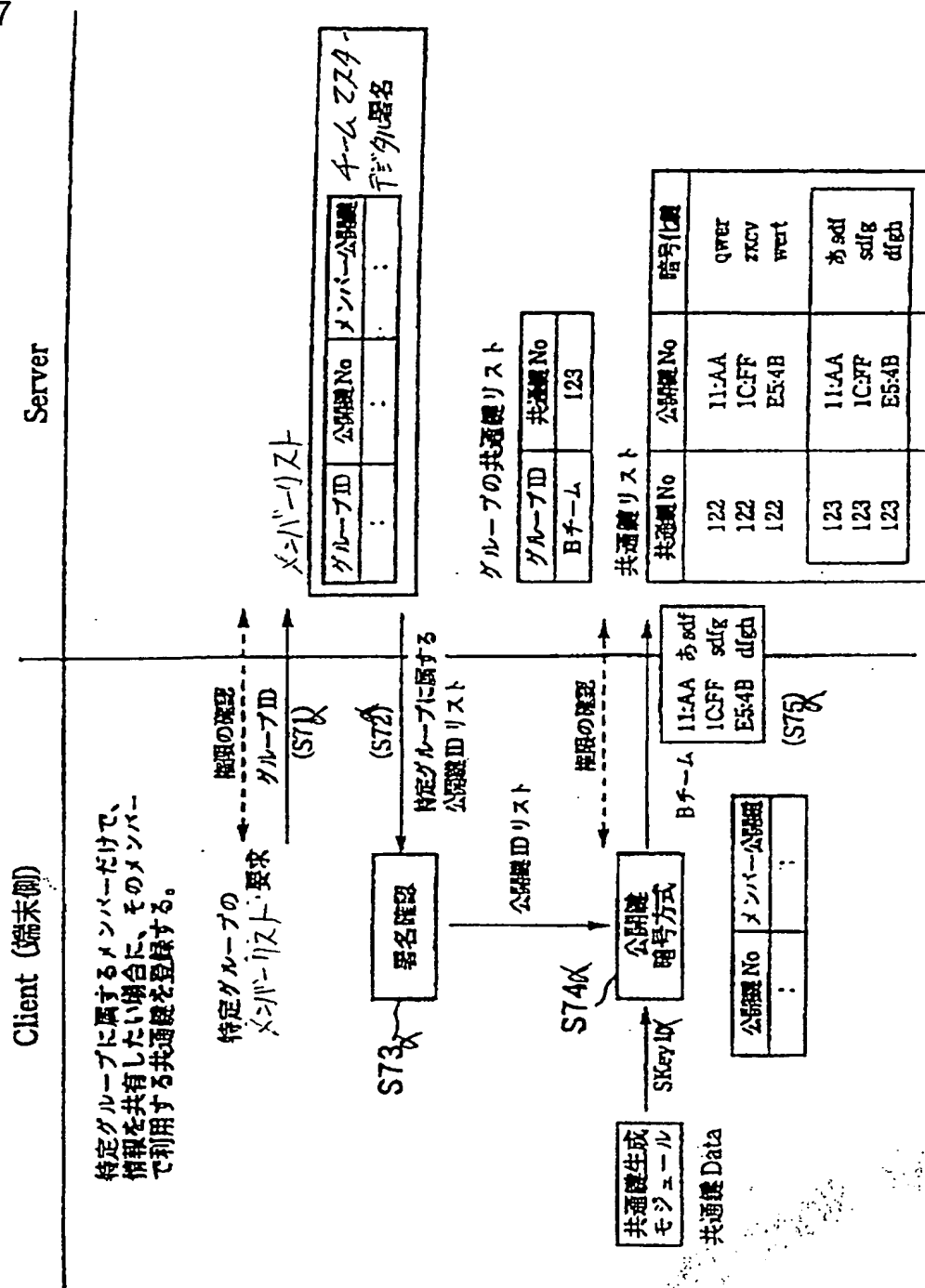
*This Page Blank (uspto)*



共通鍵の登録例（グループで共通鍵を共有する方式）

义

7



*This Page Blank (uspto)*



00

# 暗号化例 (グループで共通鍵を共有する方式)

Client (端末側)

Server

特定グループのメンバーと情報を共有したい場合の暗号化手順

グループの共通鍵リスト

| グループID | 共通鍵No |
|--------|-------|
| Aチーム   | 122   |

共通鍵リスト

| 共通鍵No | 公開鍵No | 暗号化鍵 |
|-------|-------|------|
| 122   | 11:AA | QWER |
| 122   | 1C:FF | ZXCV |
| 122   | E5:4B | WERT |

特定グループの  
共通鍵要求

情報の確認  
グループID

ユーザ公開鍵No  
(S81)

S83  
公開鍵  
暗号方式

122 ZXCV  
(S82)

グループで利用する共通鍵  
SK<sub>grp2</sub> (S84)

データ  
こんにちは

共通鍵  
暗号方式

S85

暗号化データ  
iiiiiiiiiii  
(S88)

データID 122

| データID | 暗号化データ      |
|-------|-------------|
| 4444  | iiiiiiiiiii |

| データID | 共通鍵No |
|-------|-------|
| 4444  | 122   |

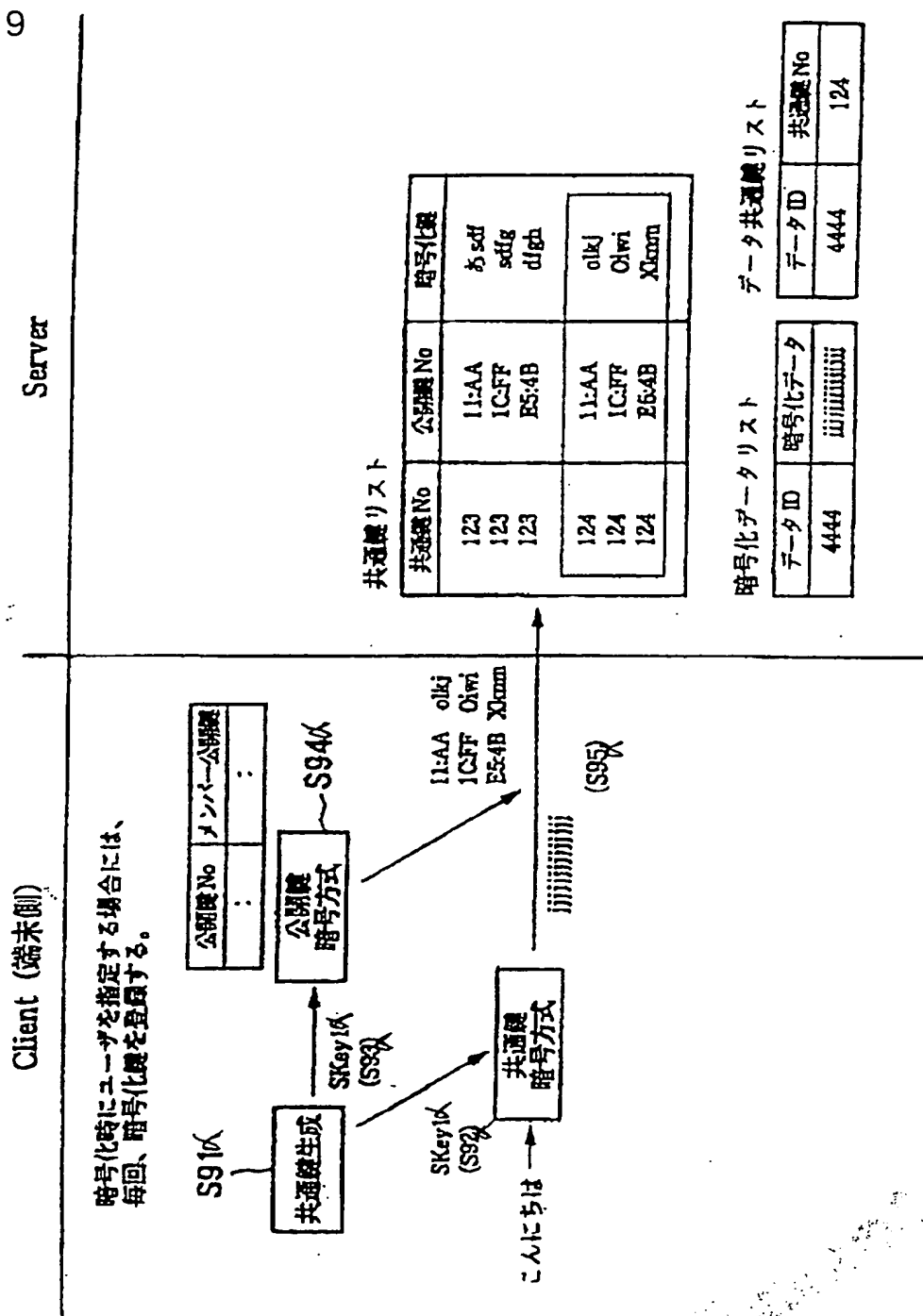
2000年10月10日

*This Page Blank (uspto)*

9/7 3

図 9

暗号化例（共有したいユーザを別途指定する方式）

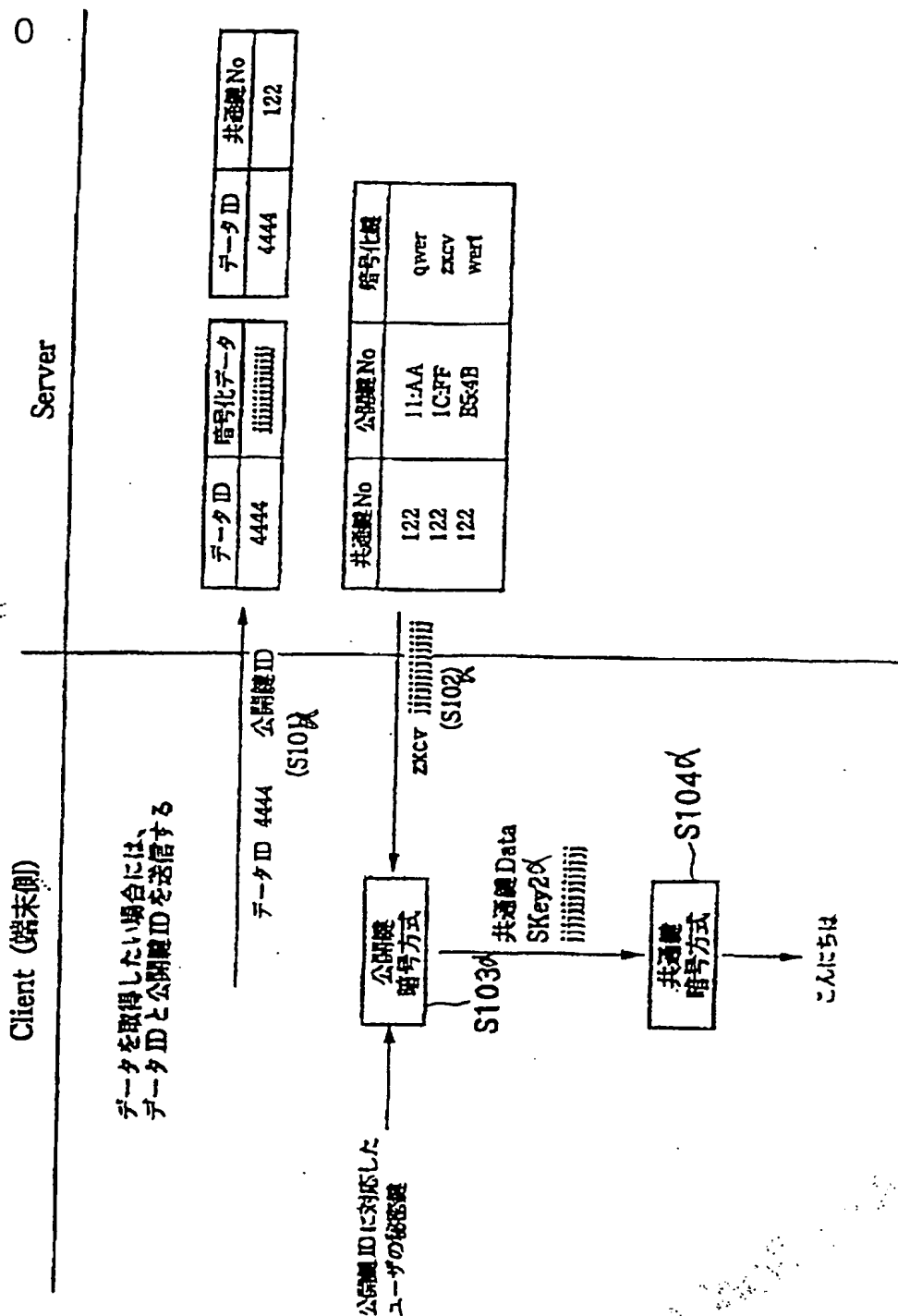


*This Page Blank (usp10)*

10/7 3

図 10

復号化例 (両方式共通)



*This Page Blank (uspto)*

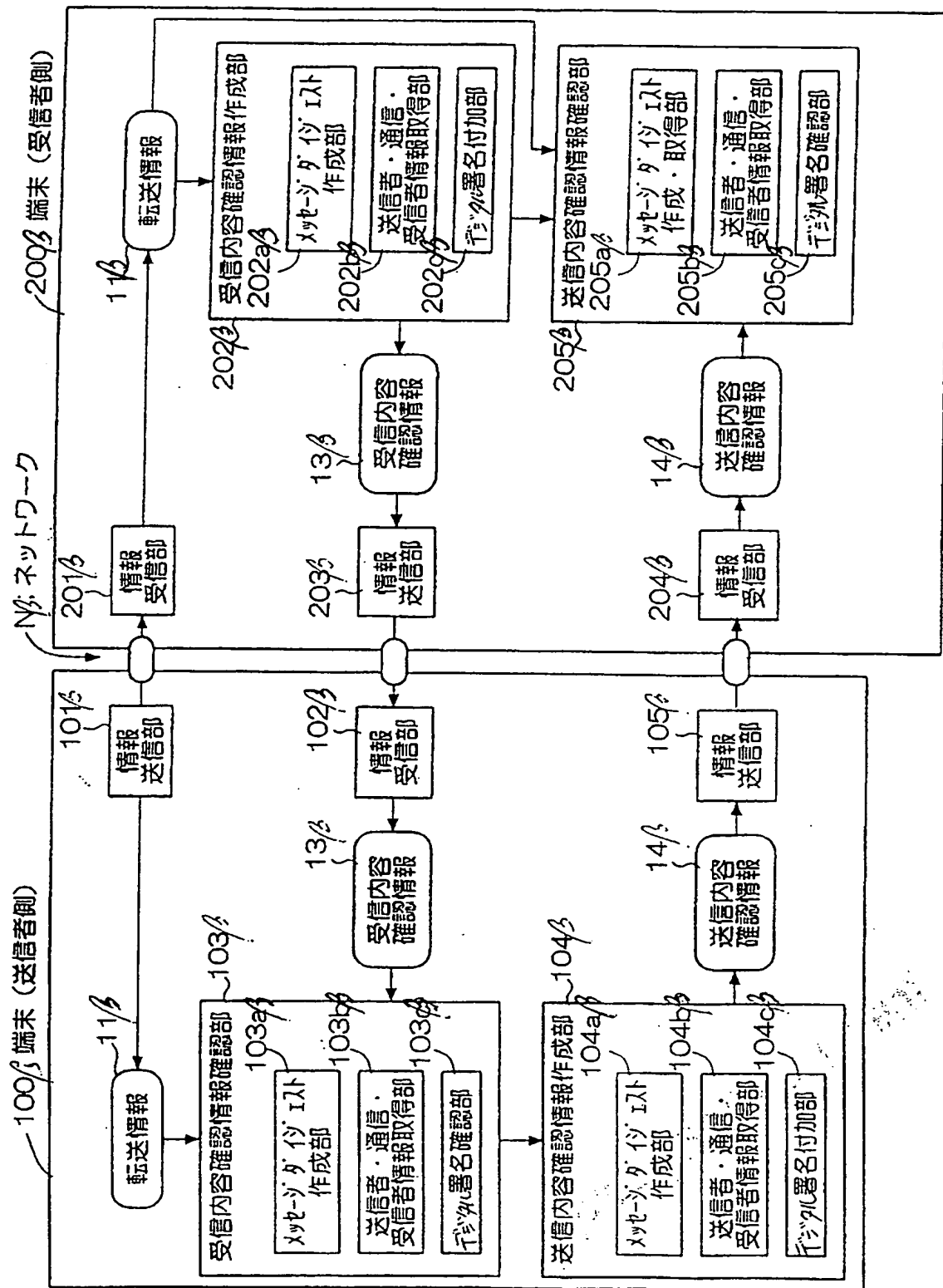




*This Page Blank (uspto)*

12/7 3

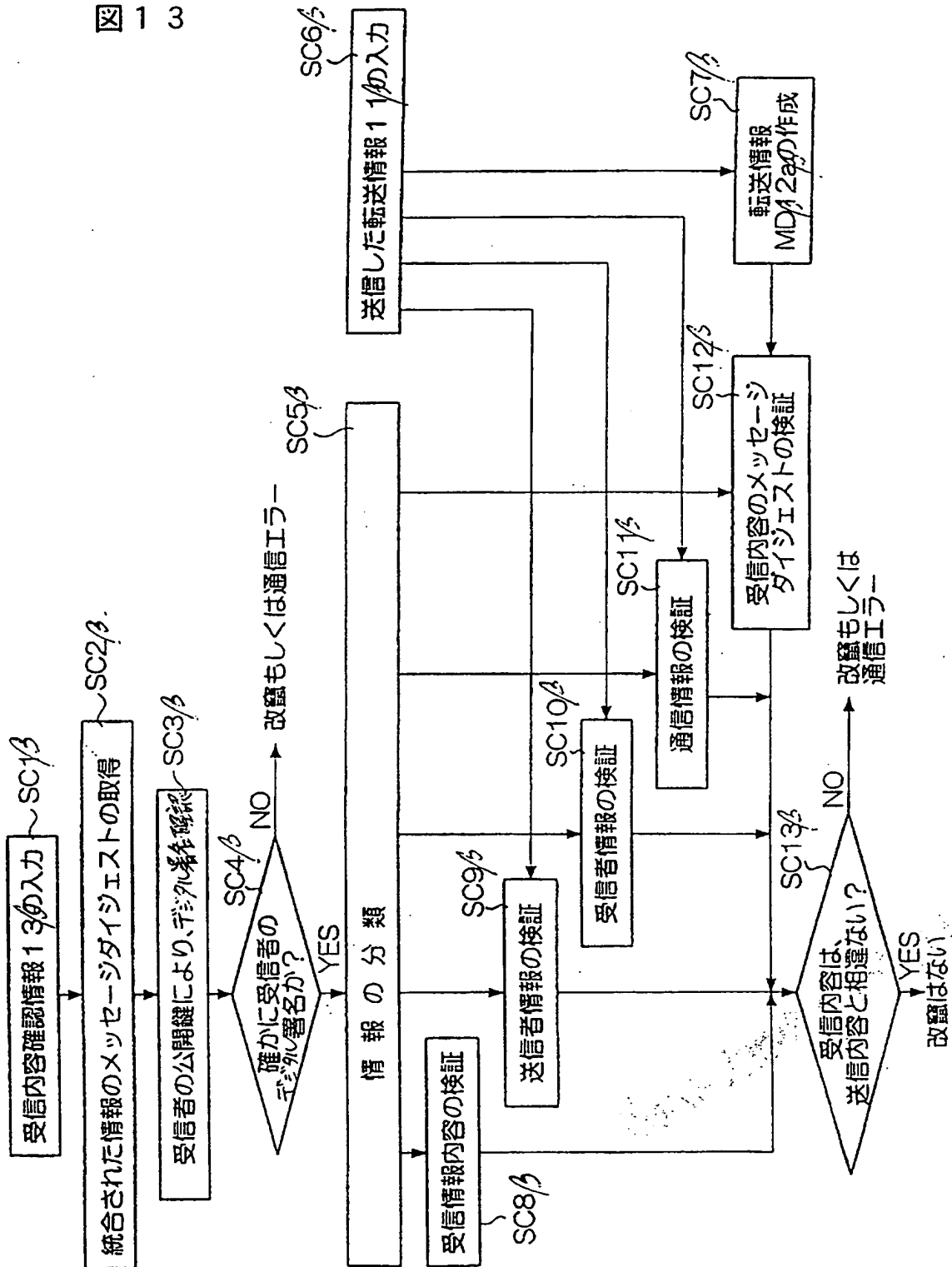
図 1 2



*This Page Blank (uspto)*

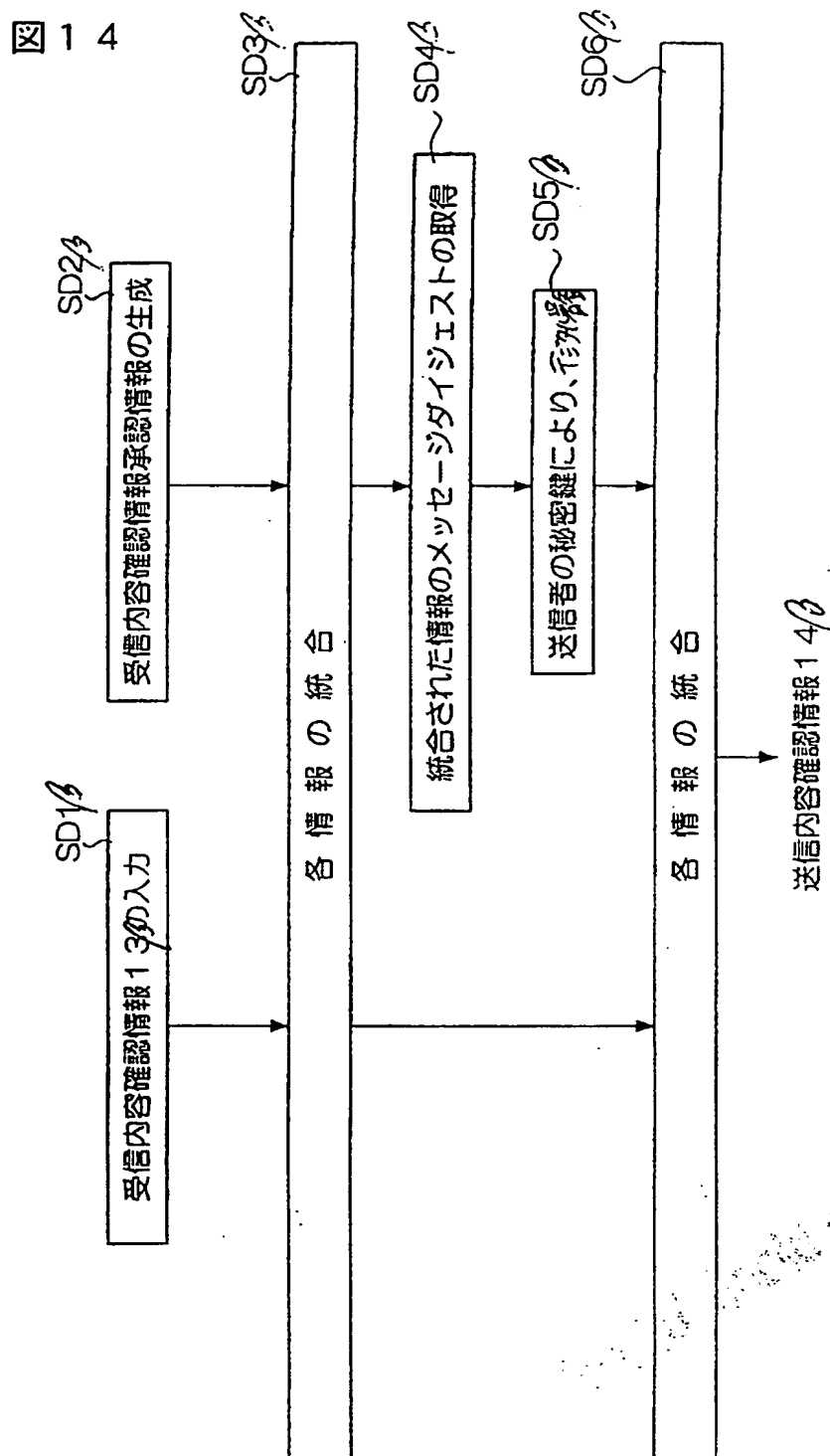
13/7 3

図 13



*This Page Blank (uspto)*

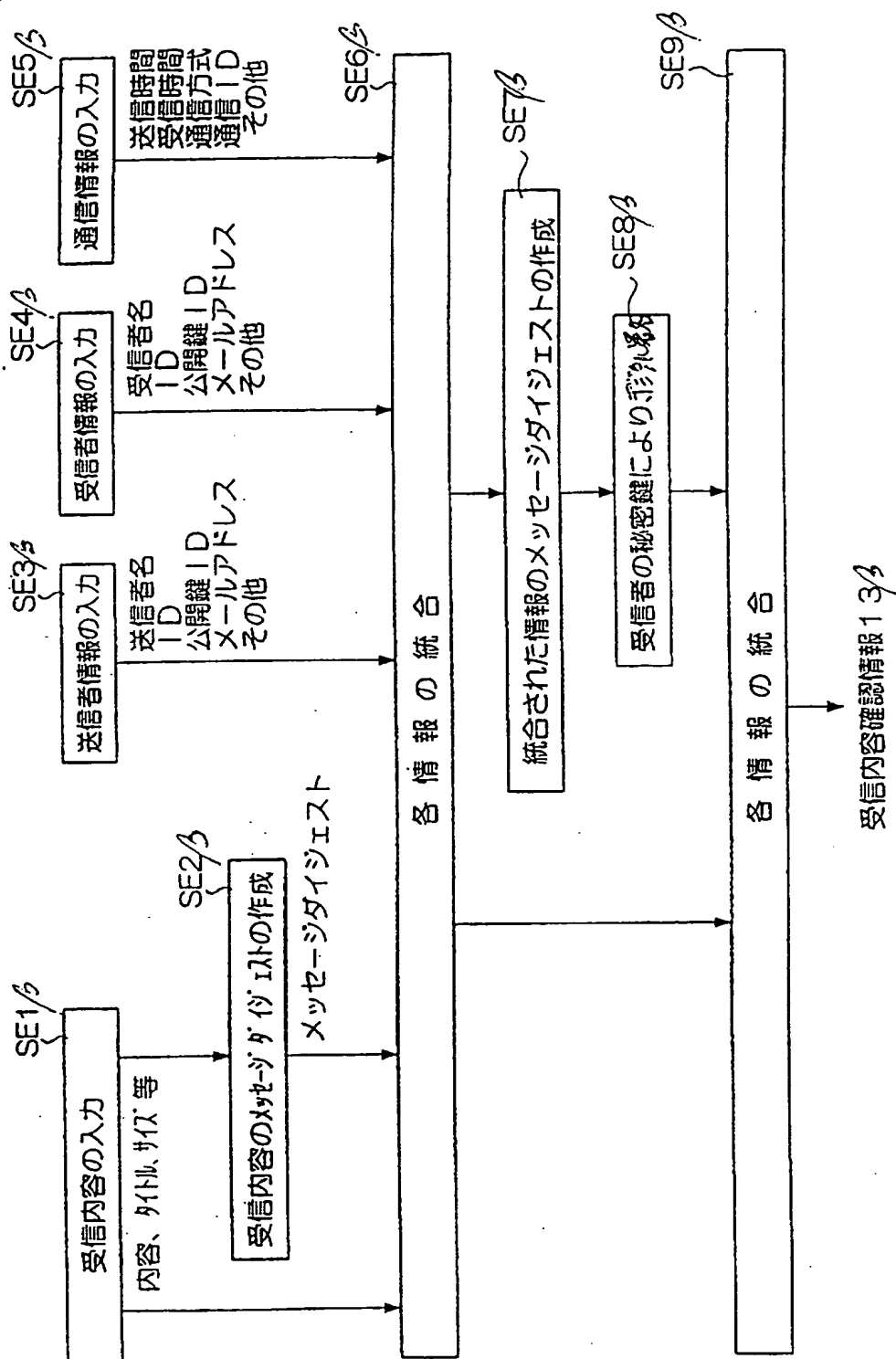
14/7 3



This Page Blank (uspto)

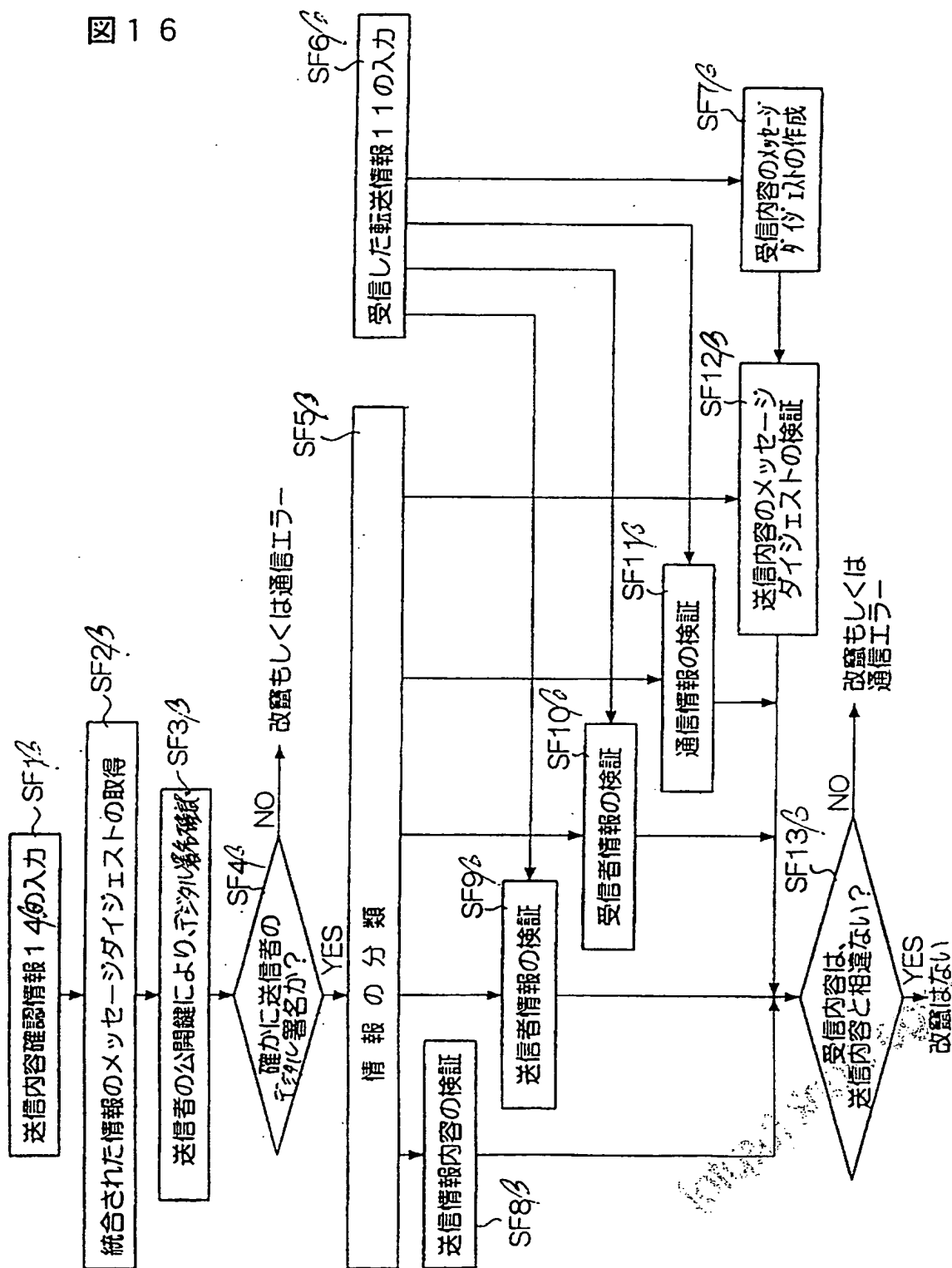


図 1 5



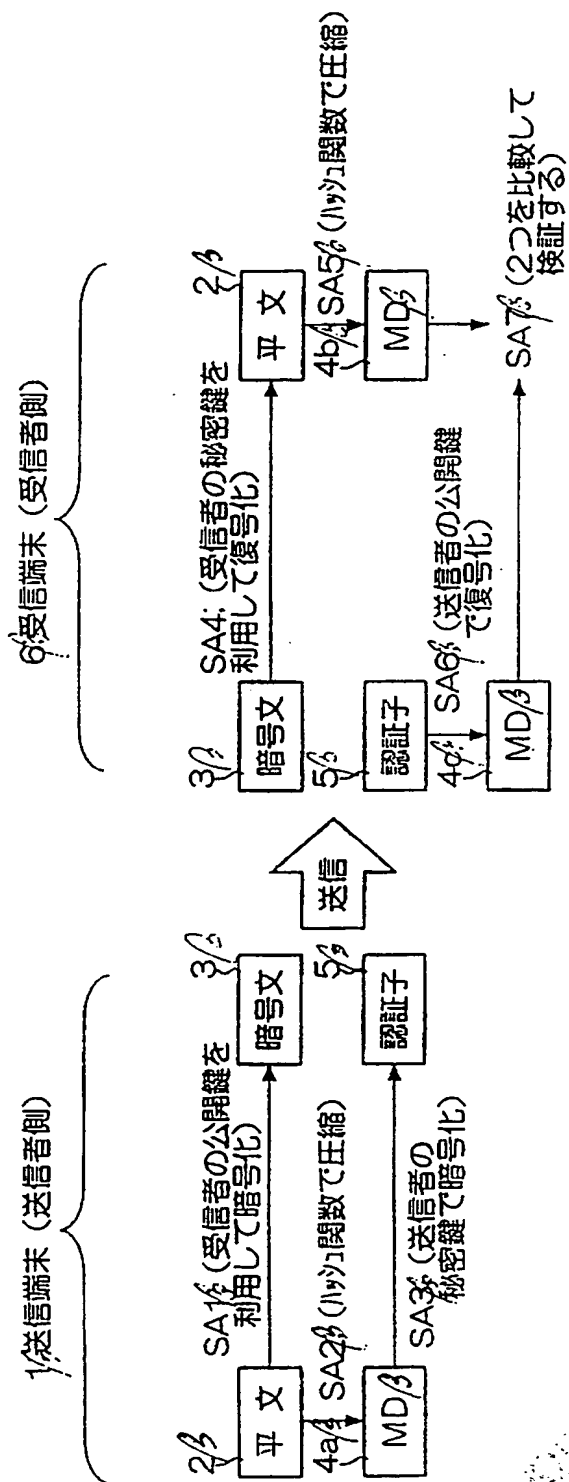
*This Page Blank (uspto)*

図 16



*This Page Blank (uspto)*

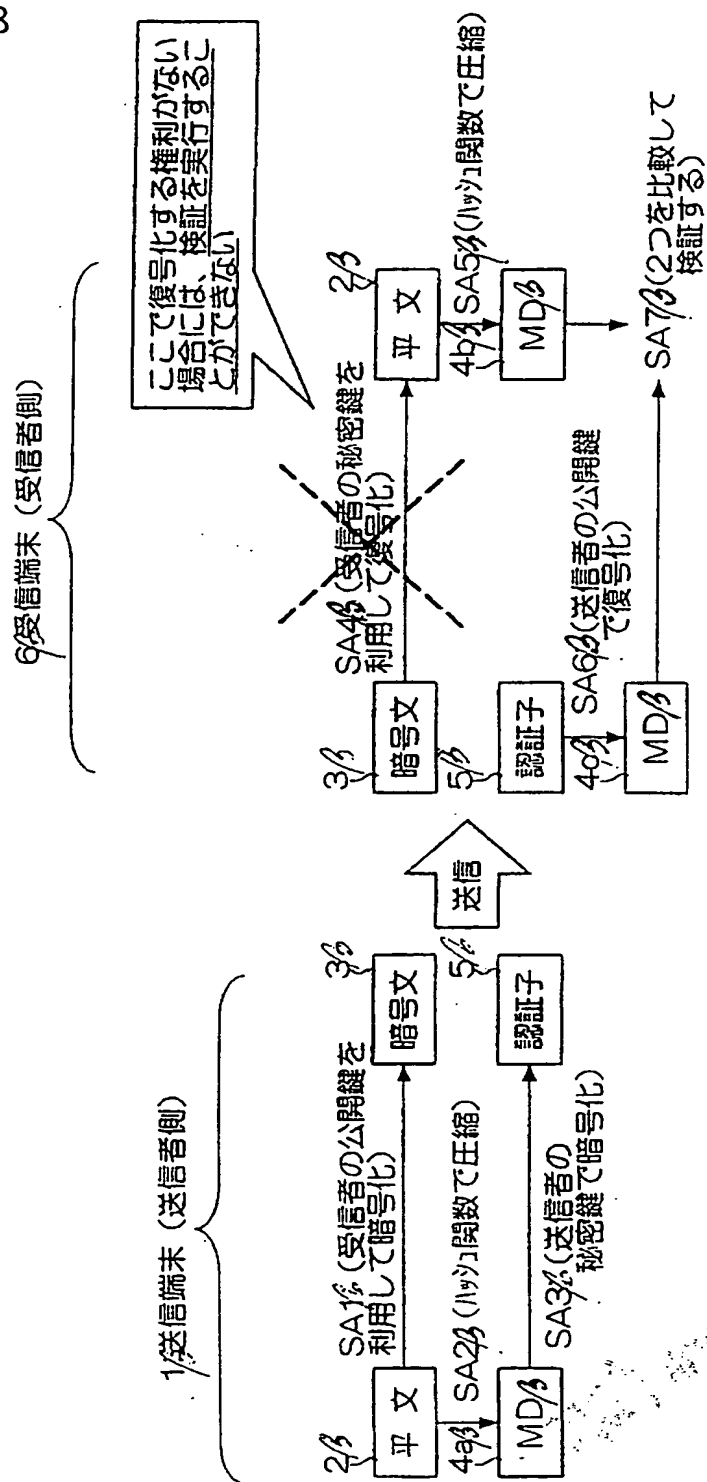
図 17



*This Page Blank (uspto)*

18/7 3

図 18

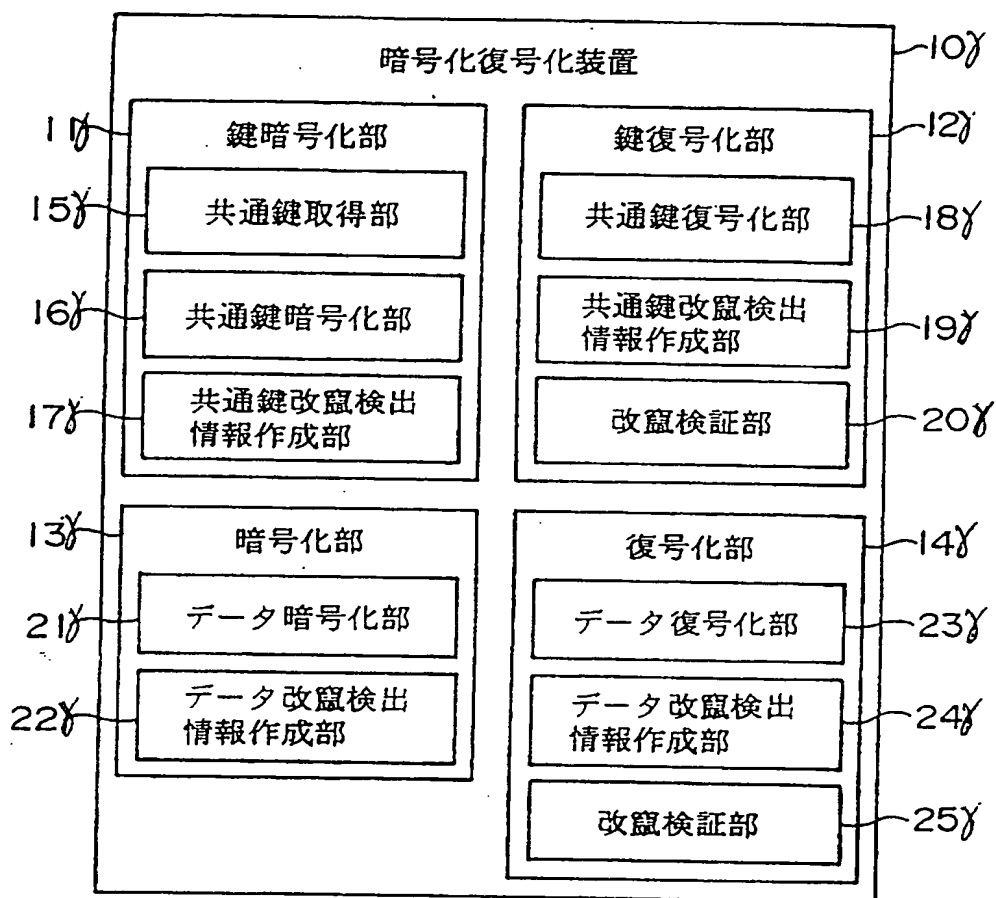


***This Page Blank (uspto)***



19/7 3

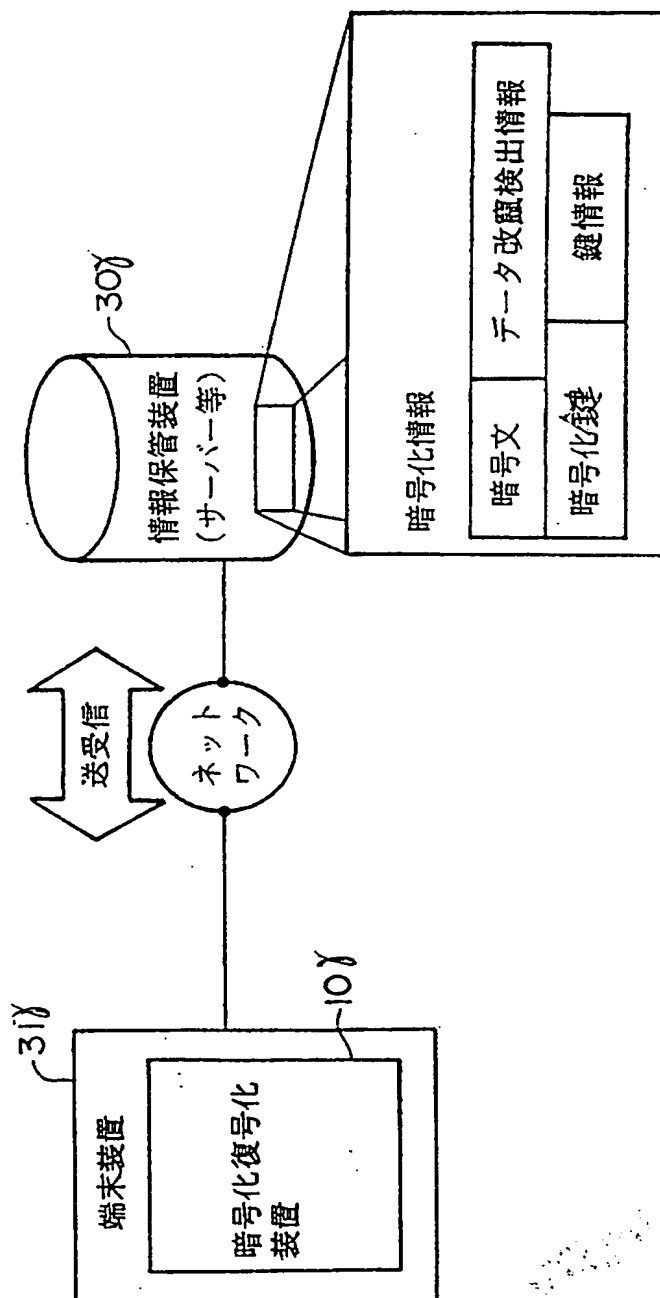
図 1 9



*This Page Blank (uspto)*

20 / 7 3

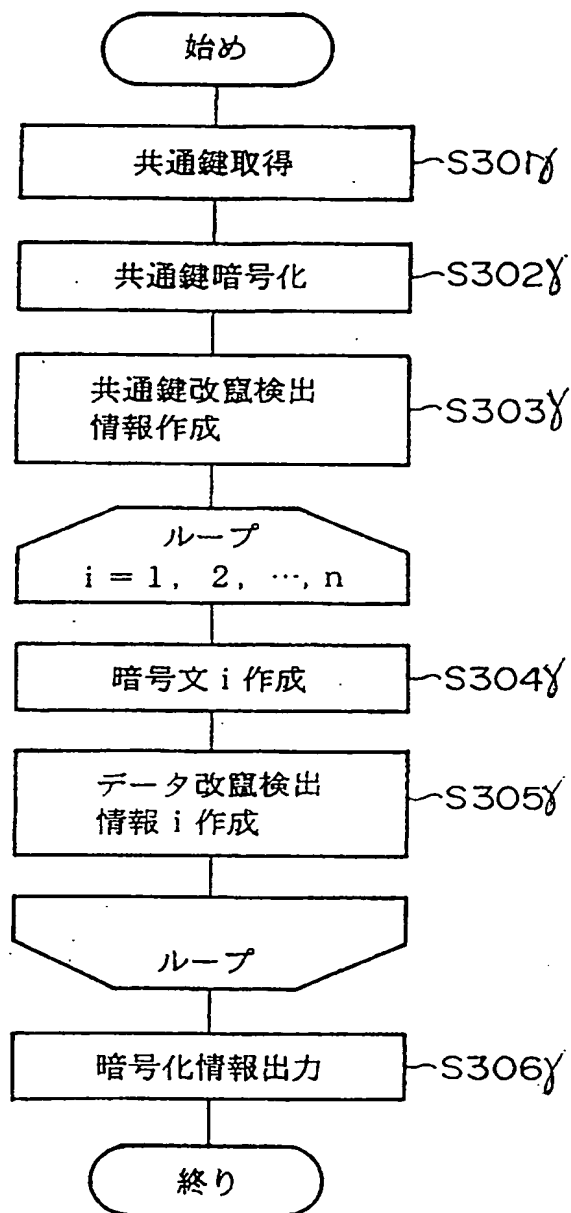
図 2 0



*This Page Blank (uspto)*

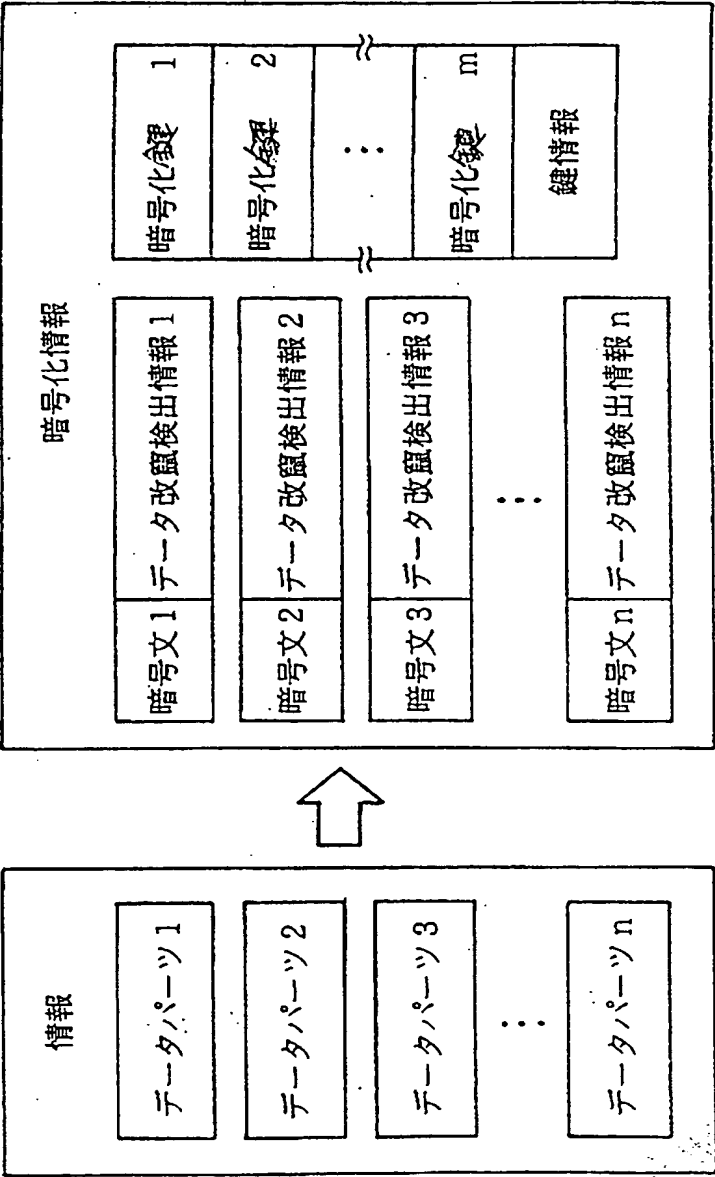
21/7 3

図 2 1



*This Page Blank (uspto)*

図 2 2

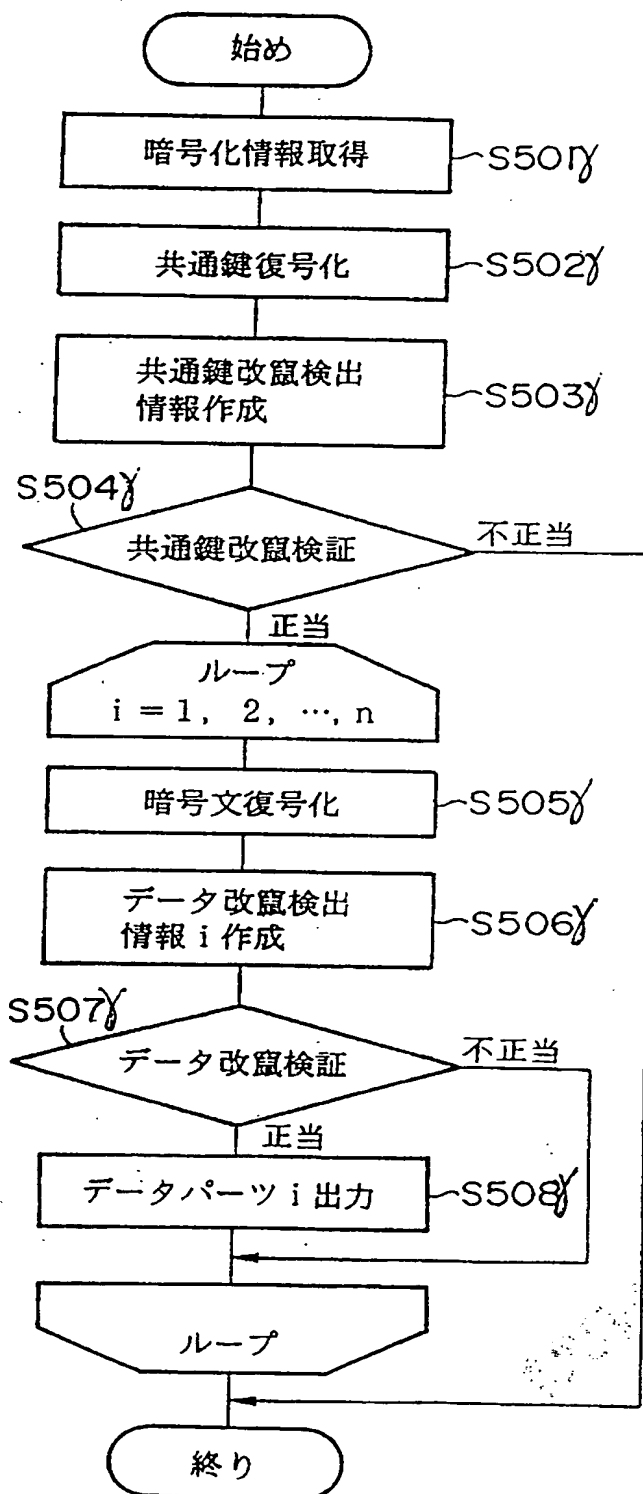


*This Page Blank (uspto)*



23 / 7 3

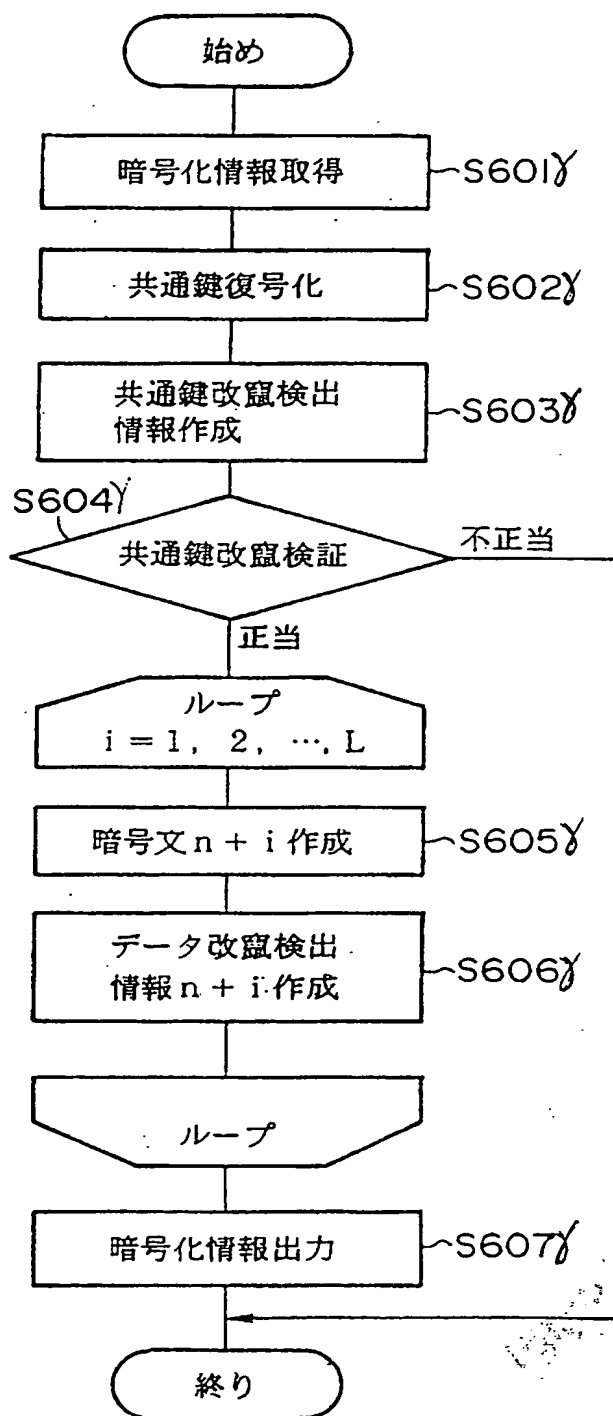
図 2 3



*This Page Blank (uspto)*

24 / 7 3

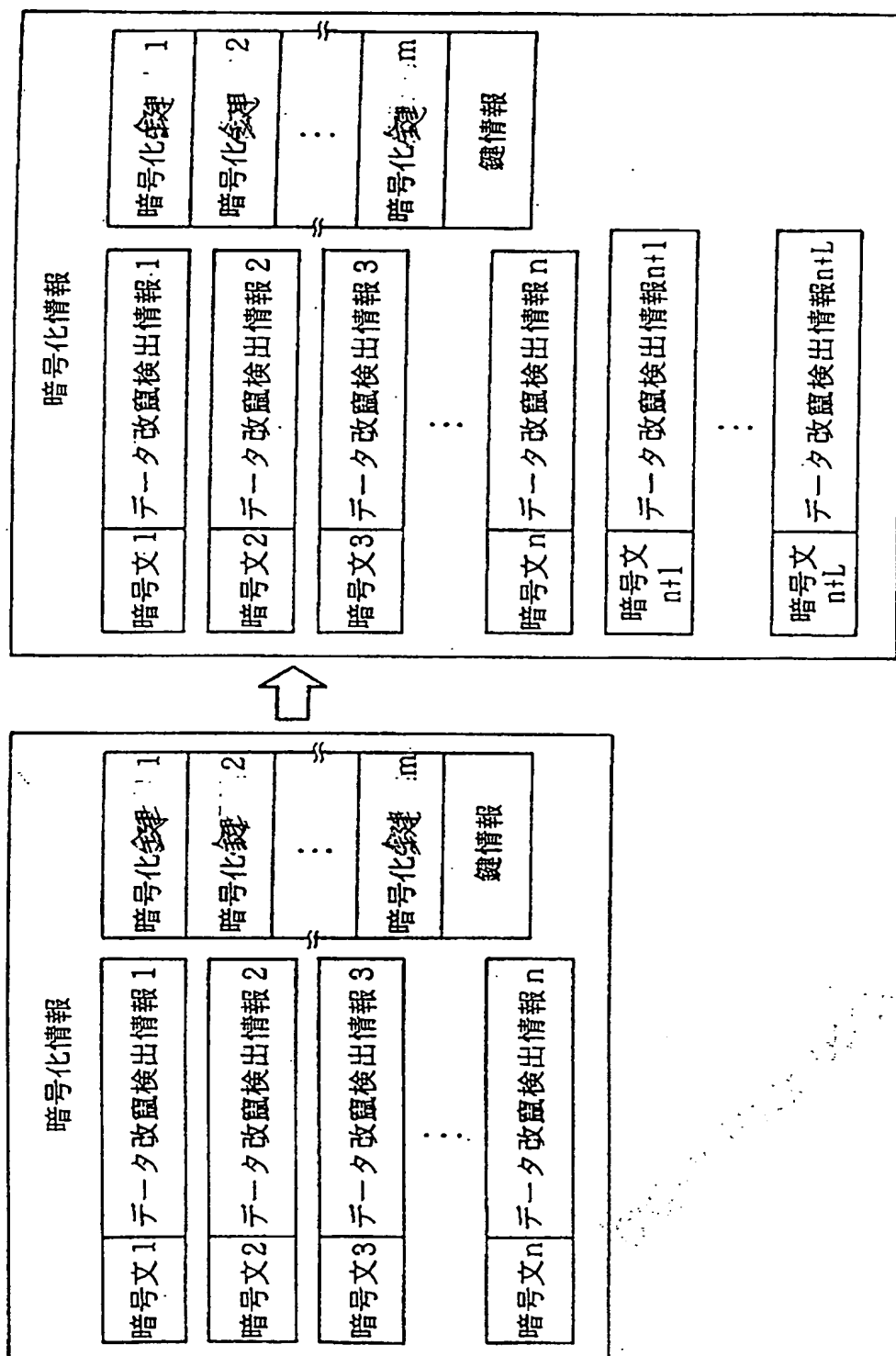
図 2 4



*This Page Blank (uspto)*

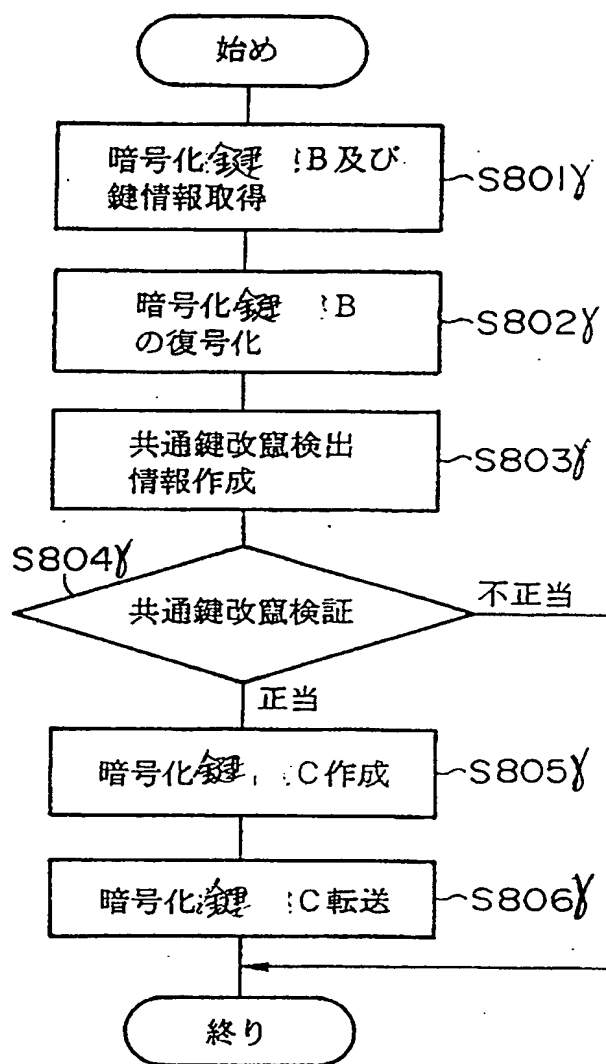
25 / 7 3

図 2 5



*This Page Blank (uspto)*

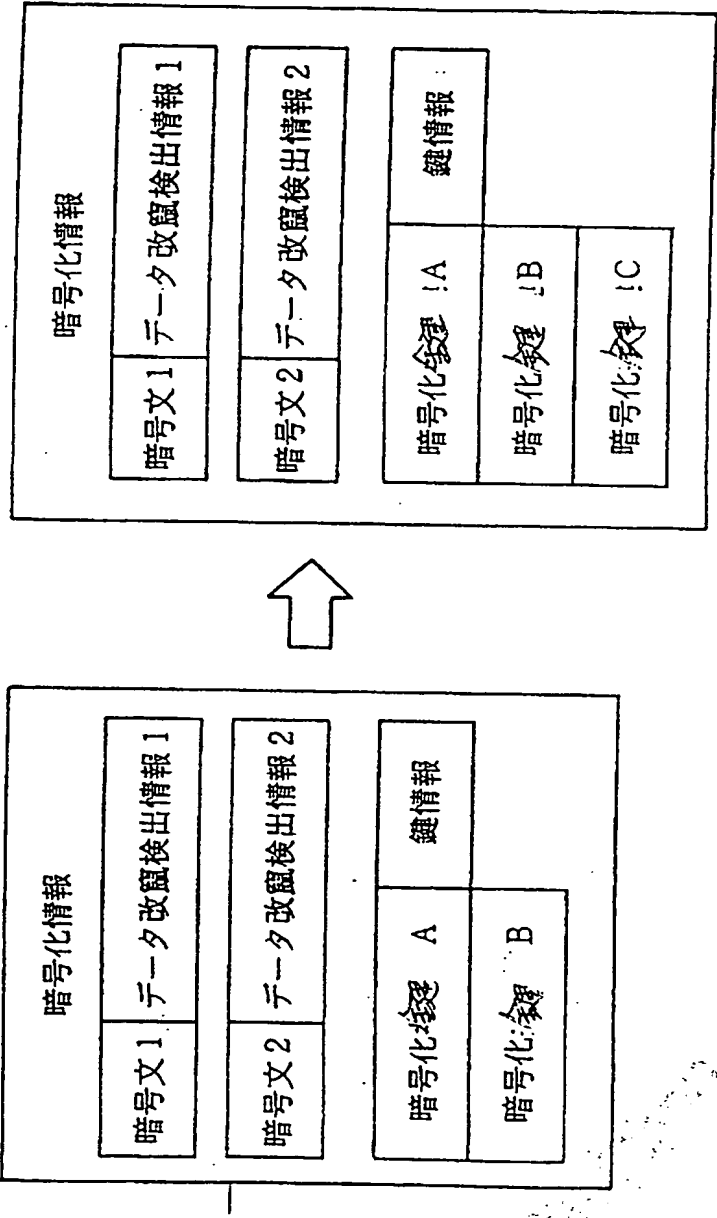
図 2 6



*This Page Blank (uspto)*



図 2 7

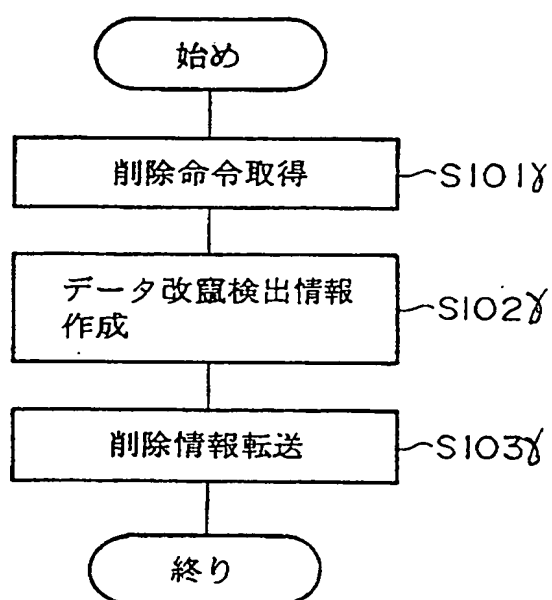


***This Page Blank (uspto)***

---

28/7 3

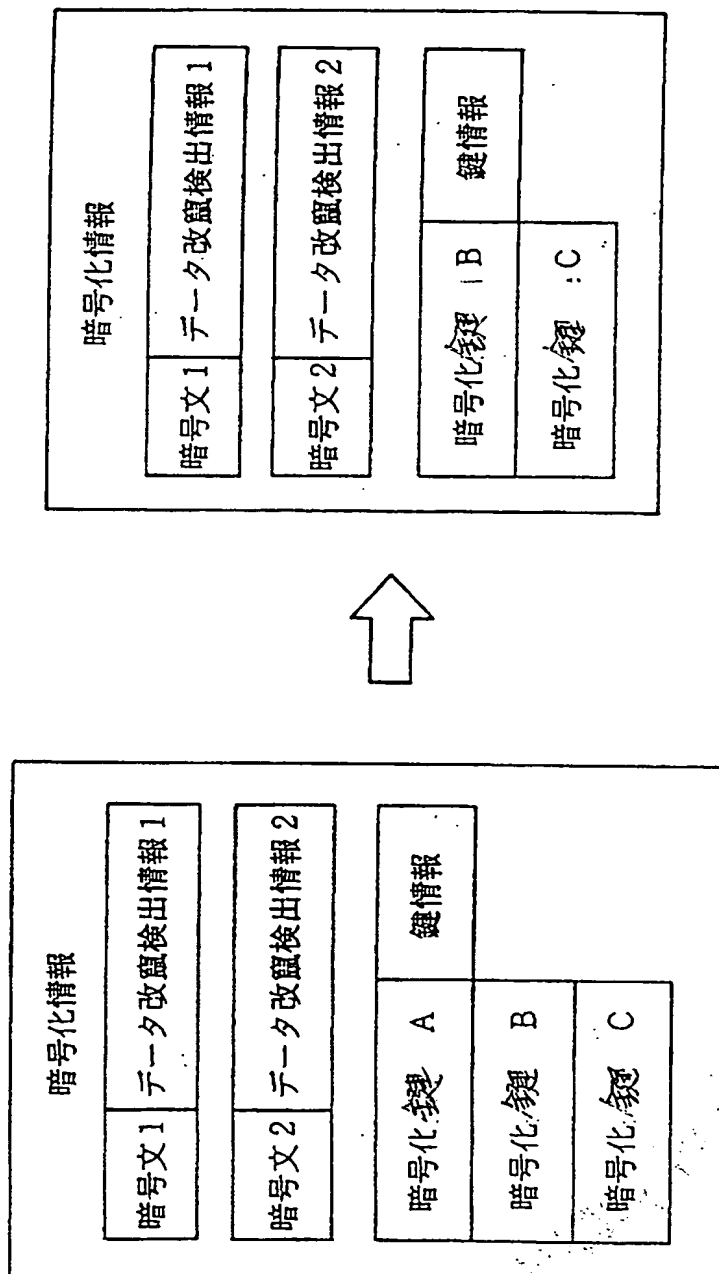
図 2 8



This Page Blank (uspto)

29/7 3

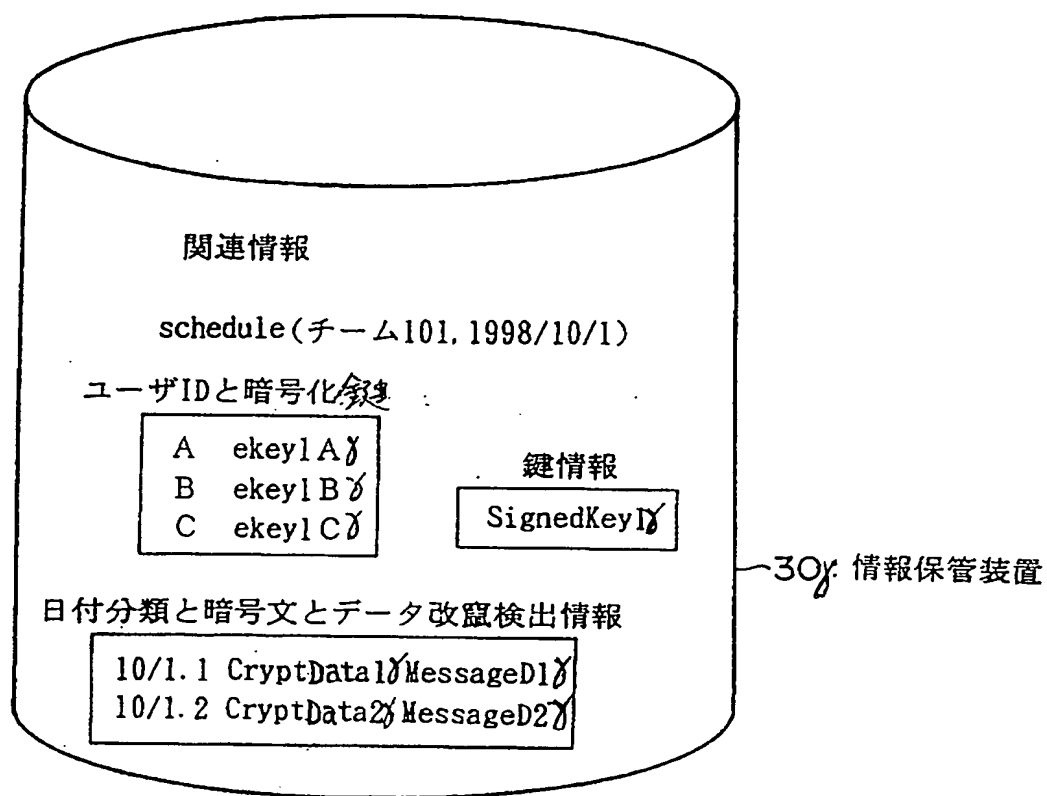
図 2 9



This Page Blank (uspto)

30/7 3

図 30

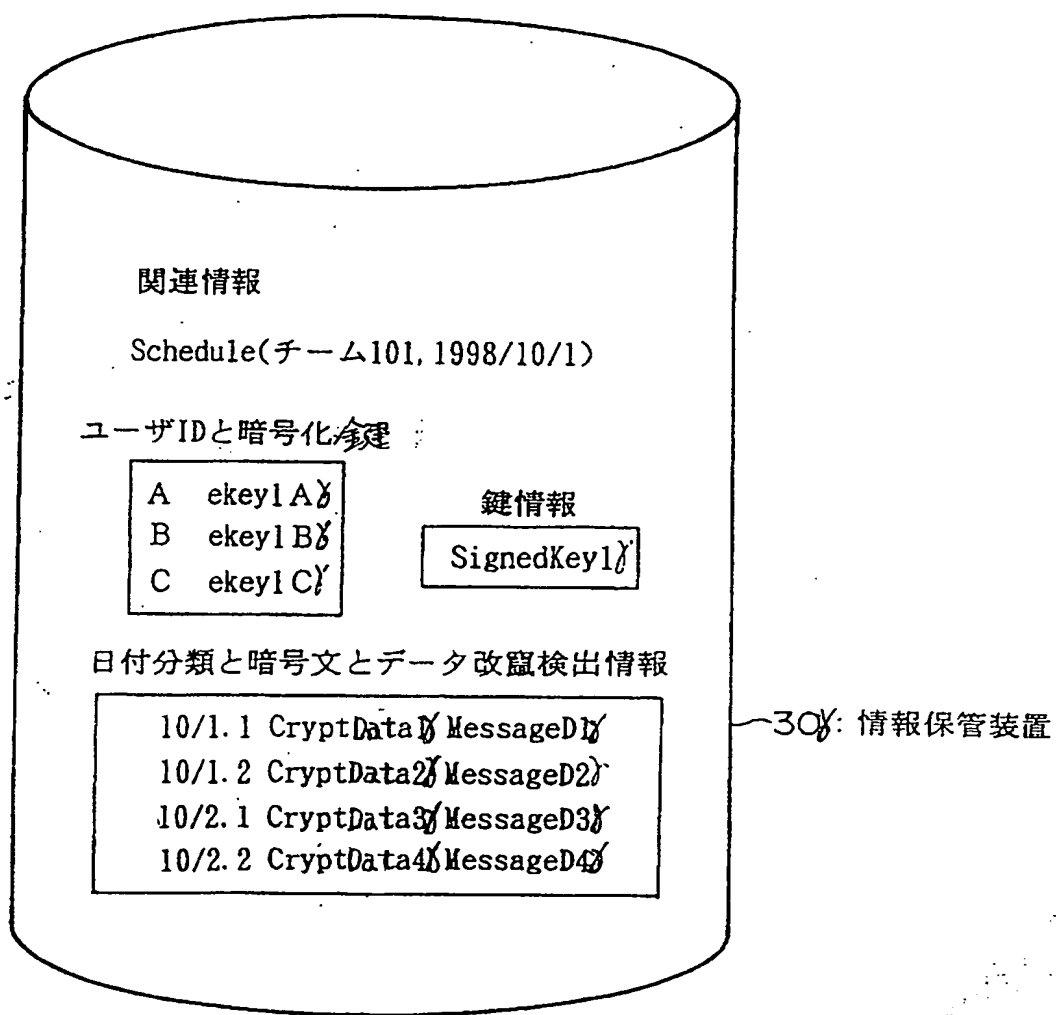


*This Page Blank (uspto)*



31/7 3

図 3 1



*This Page Blank (uspto)*

32/7 3

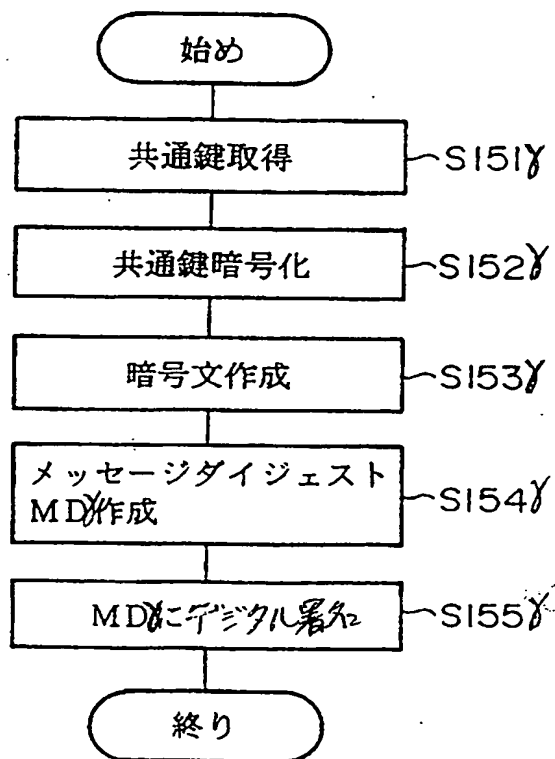
図 3 2

チーム 101 : スケジュール

10月

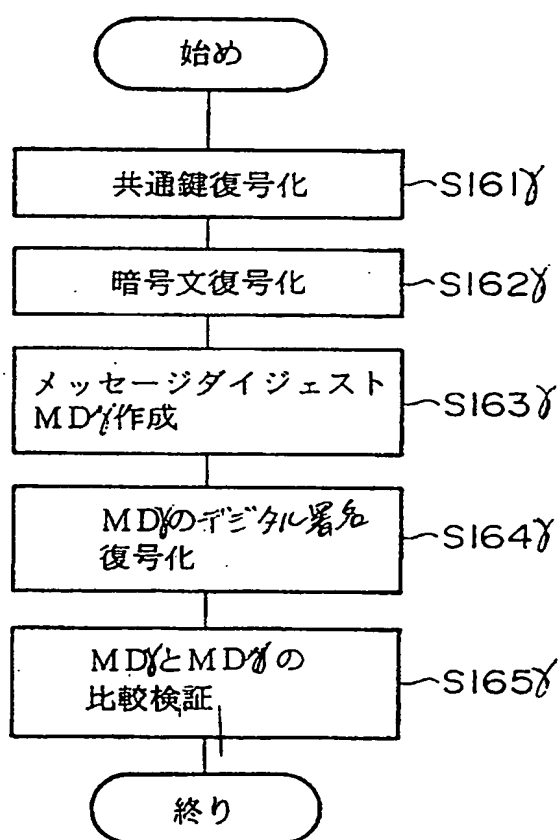
|                            |                        |  |
|----------------------------|------------------------|--|
| 1日<br>B : セミナー参加<br>15:00~ | 2日<br>A : 会議<br>17:00~ |  |
|                            |                        |  |

図 3 3



*This Page Blank (uspto)*

図 3 4



*This Page Blank (uspto)*

図 3 5

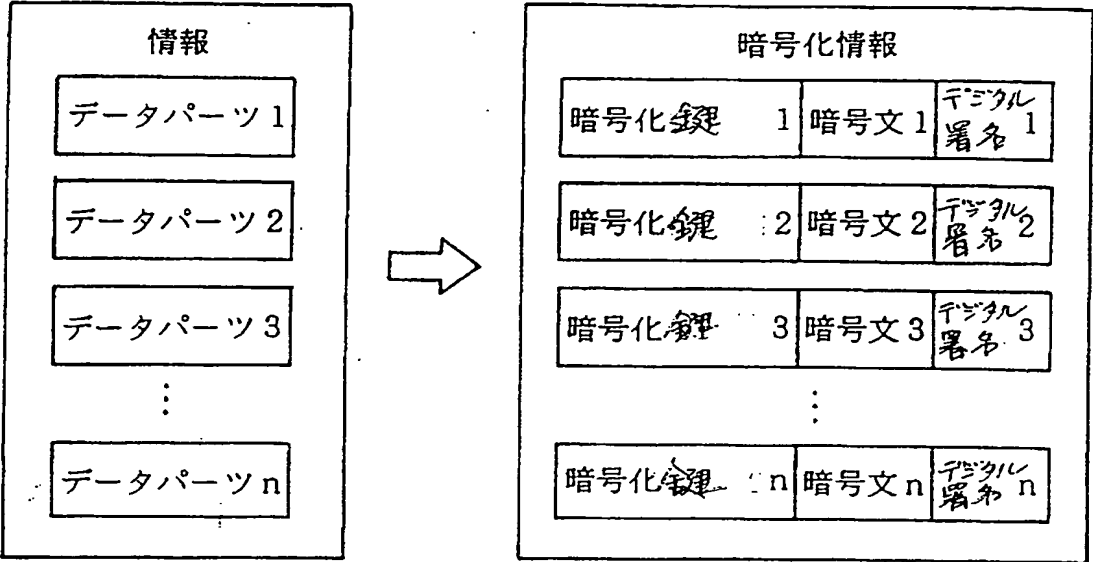
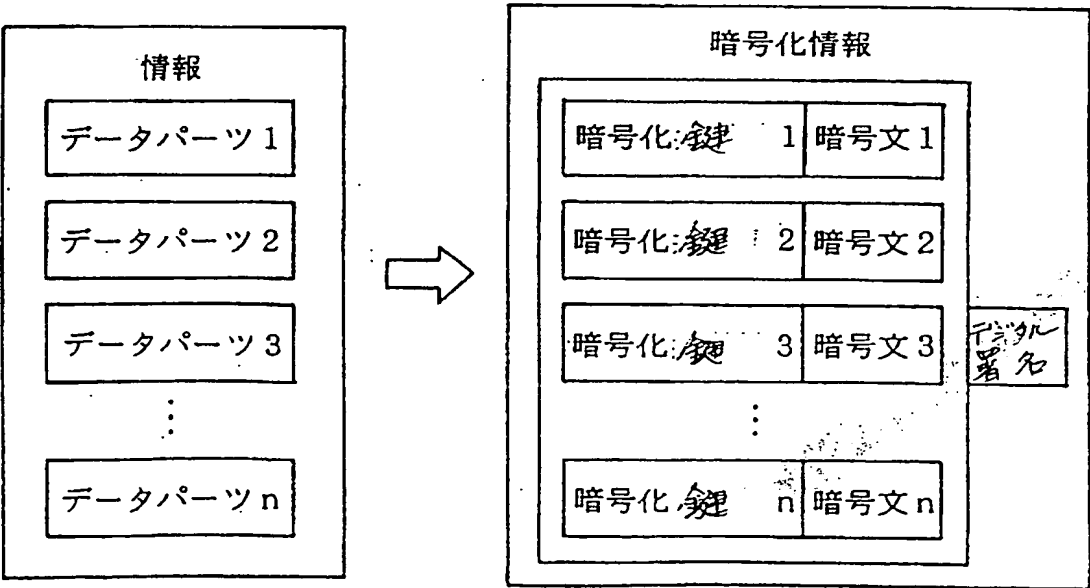


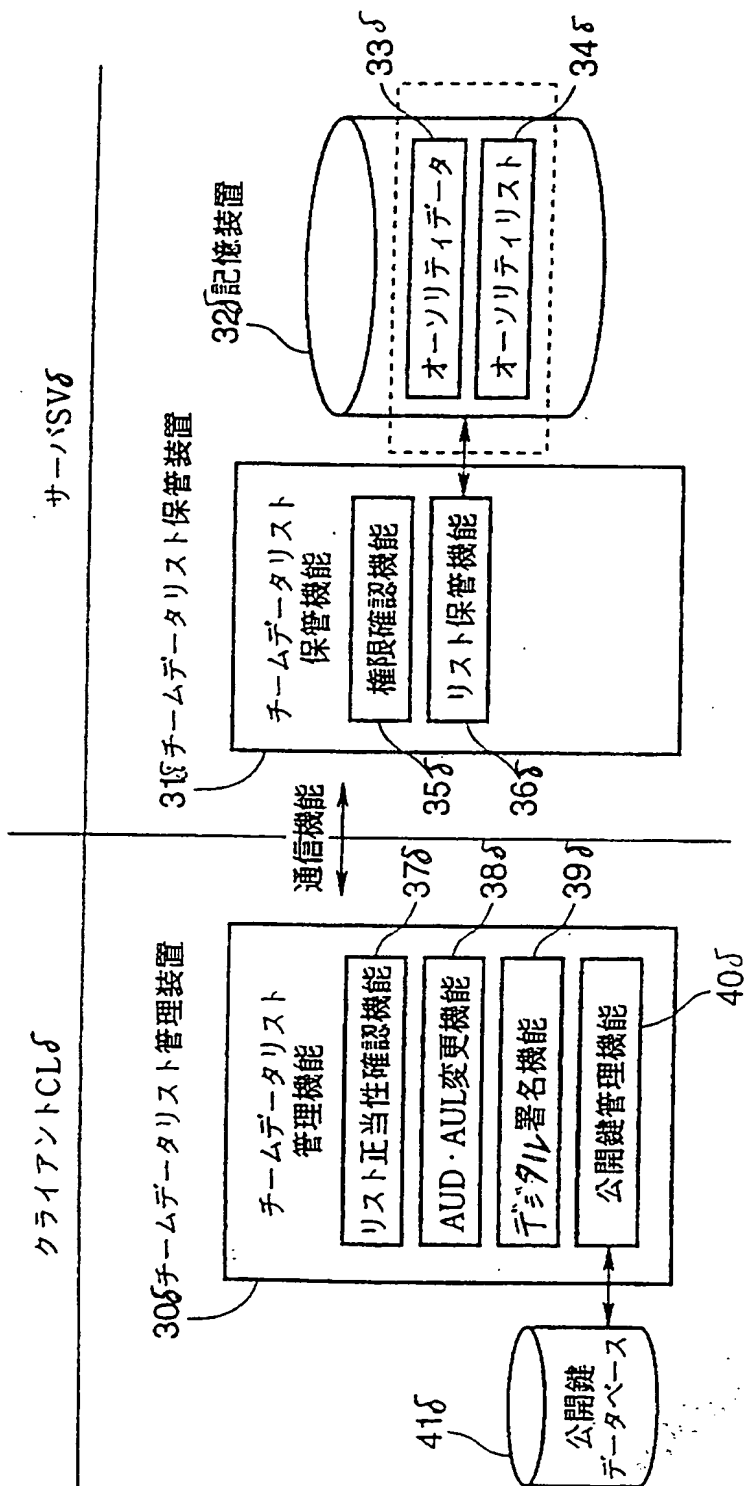
図 3 6



*This Page Blank (uspto)*



図 3 7



*This Page Blank (uspto)*

図 3 8 A

|          |       |      |
|----------|-------|------|
| AUDδ     |       | 33   |
| チームID    | 103   |      |
| 親チームID   | 101   |      |
| チーム作成者   | メンバーB |      |
| チームマスタ   | メンバーX |      |
| Bのデジタル署名 |       | 33eδ |

図 3 8 B

|          |       |      |
|----------|-------|------|
| AUDδ     |       | 34δ  |
| チームID    | 103   |      |
| チームマスタ   | メンバーX |      |
| サブオーソリテイ | メンバーC |      |
| サブオーソリテイ | メンバーD |      |
| Xのデジタル署名 |       | 34eδ |

図 3 8 C

|               |     |           |  |
|---------------|-----|-----------|--|
| AUDδ          | B署名 | 33cδ 33eδ |  |
|               |     | 33bδ 33aδ |  |
| 101/102, TM=X |     | 33d       |  |
|               |     |           |  |

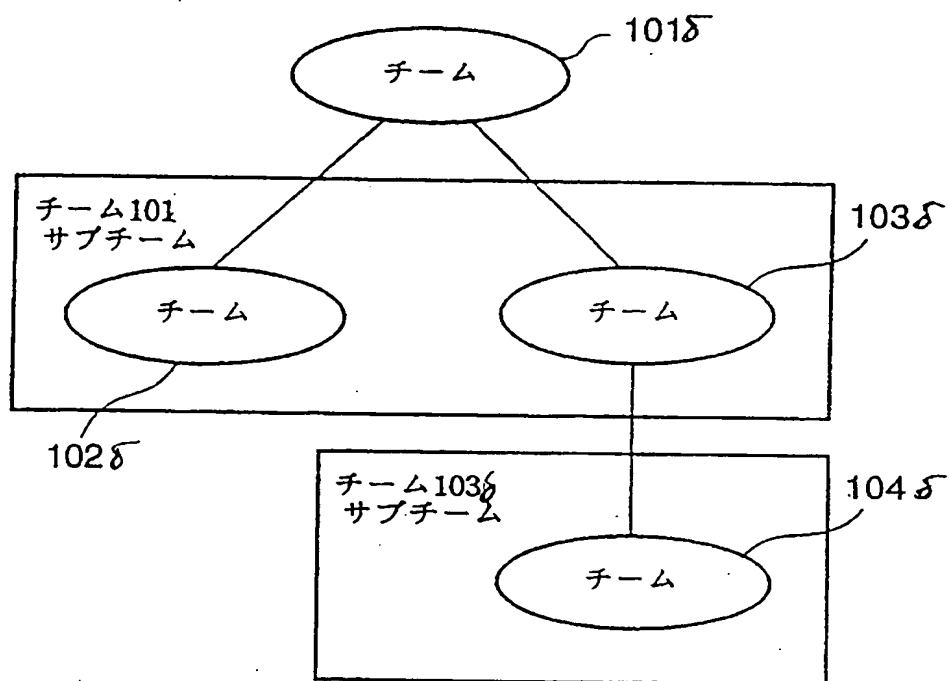
図 3 8 D

|      |      |                   |
|------|------|-------------------|
| AULδ | X署名  | TMδX, subAUDδC, D |
| 34dδ | 34bδ | 34cδ              |

*This Page Blank (uspto)*

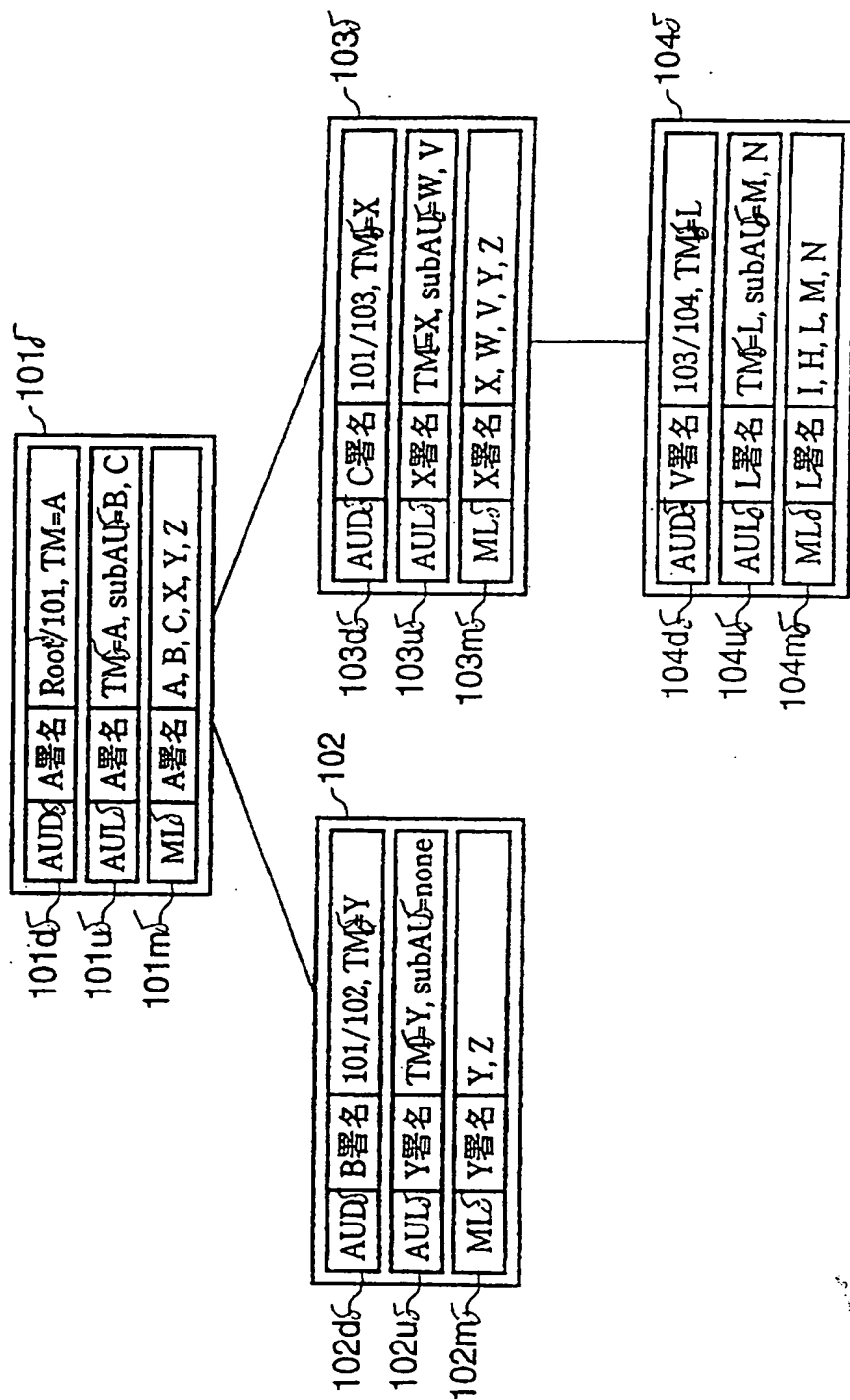
37/7 3

図 3 9



*This Page Blank*

図 4 0

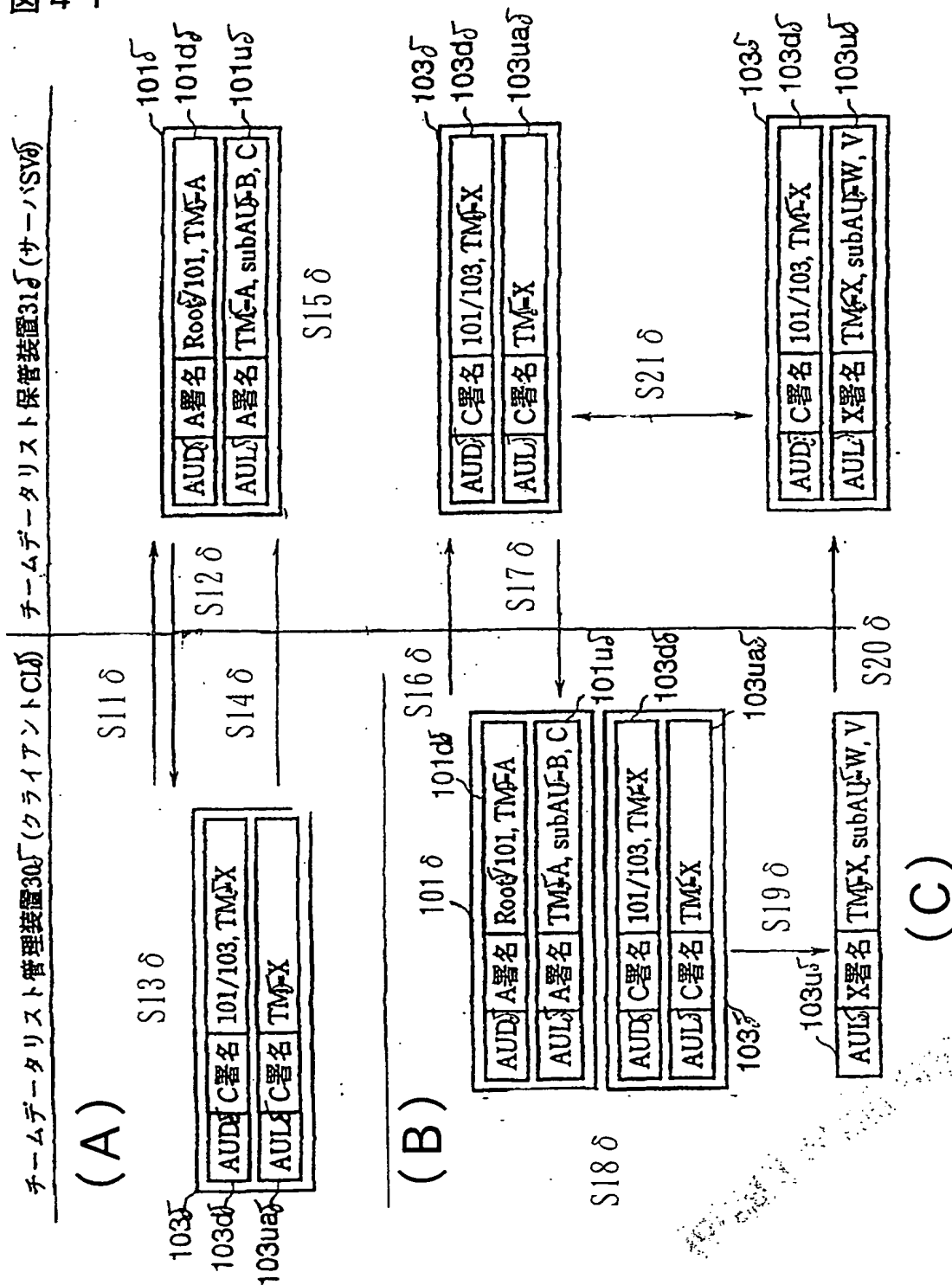


*This Page Blank (uspto)*



39 / 73

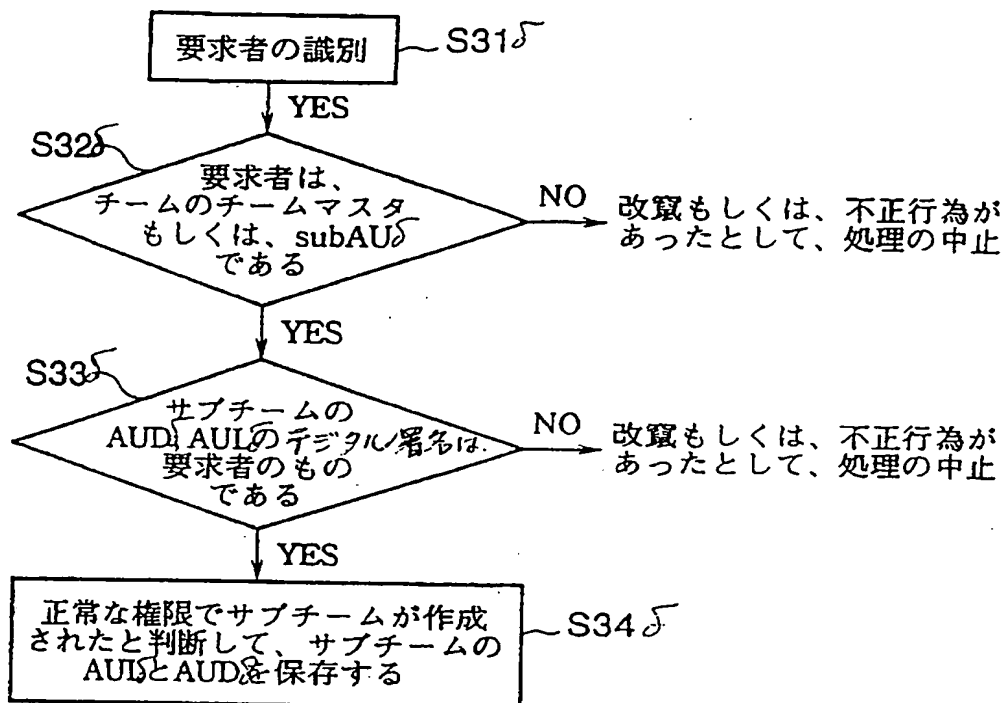
図 4 1



*This Page Blank (uspto)*

40/73

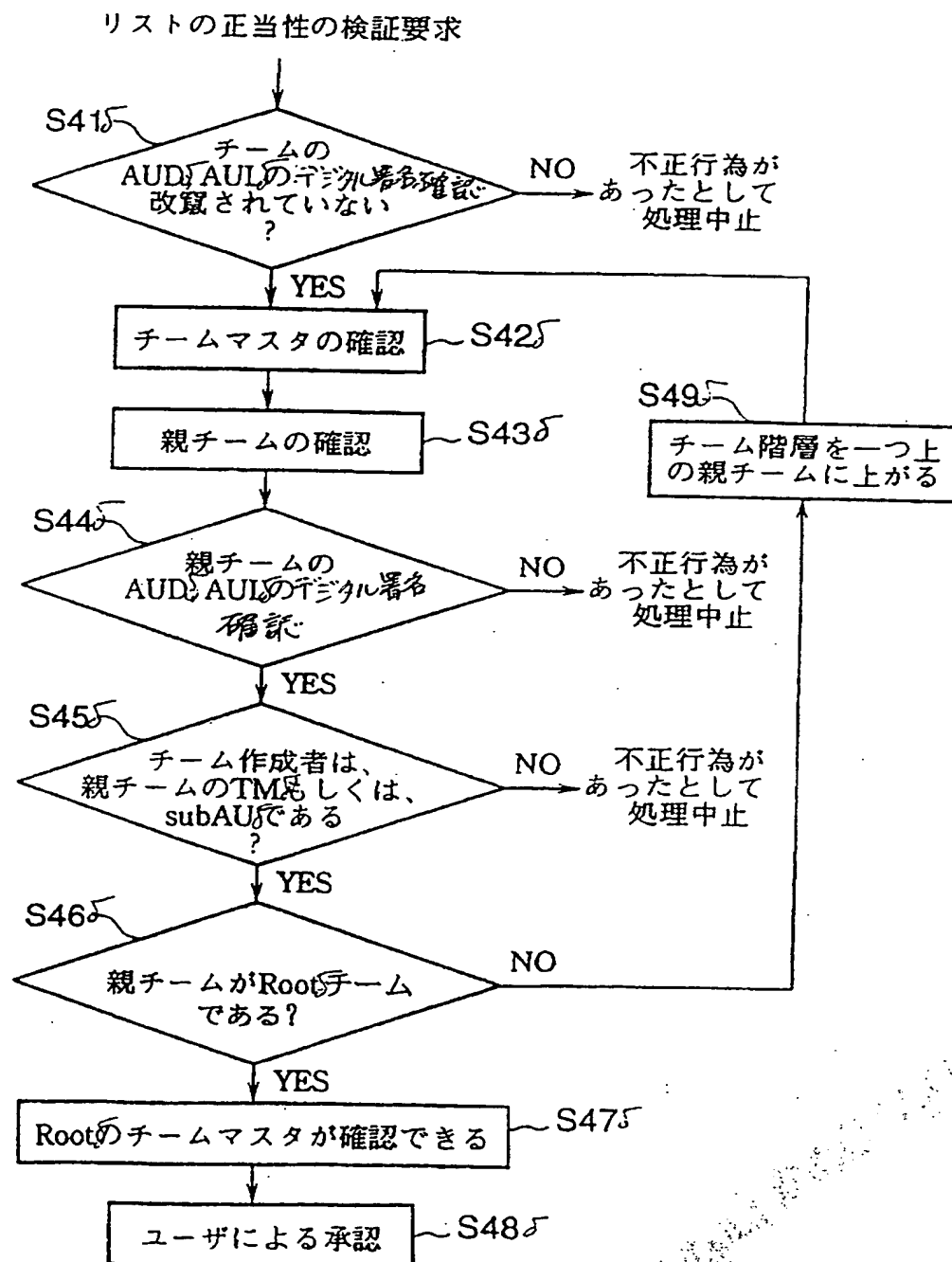
図 4 2



*This Page Blank (uspto)*

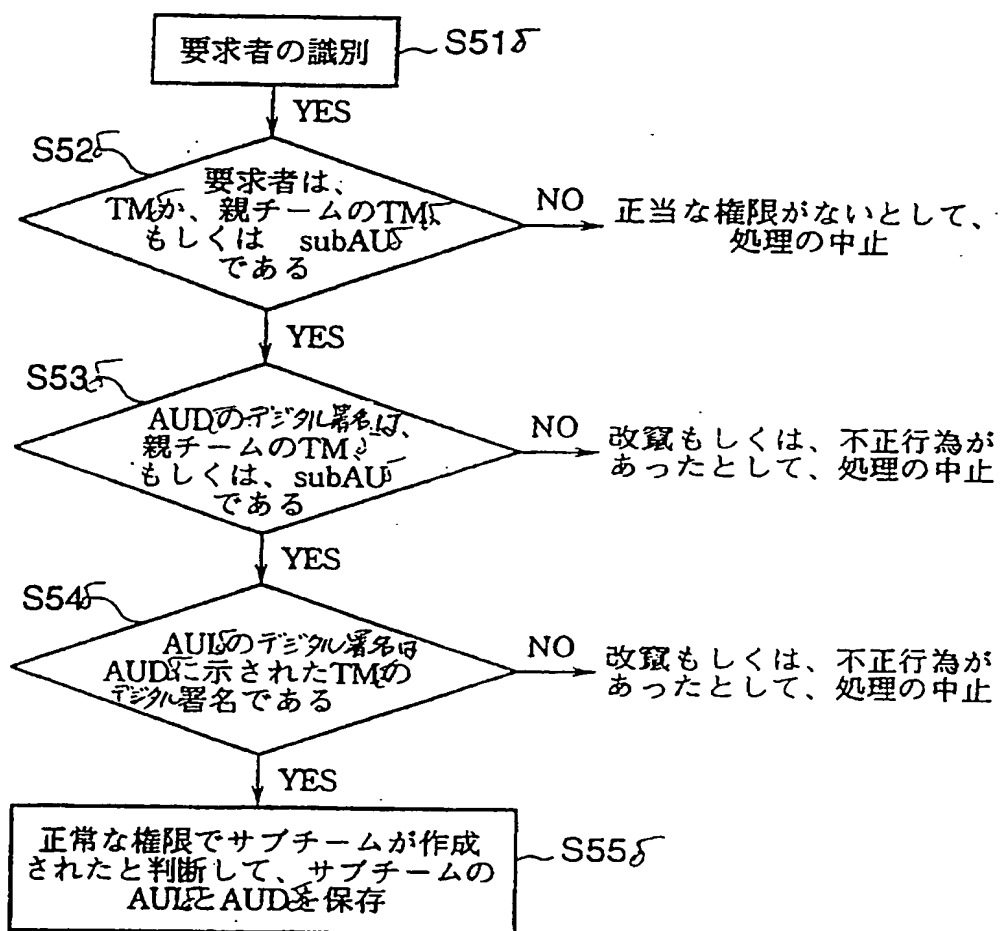
41/73

図 4 3



*This Page Blank (uspto)*

図 4 4

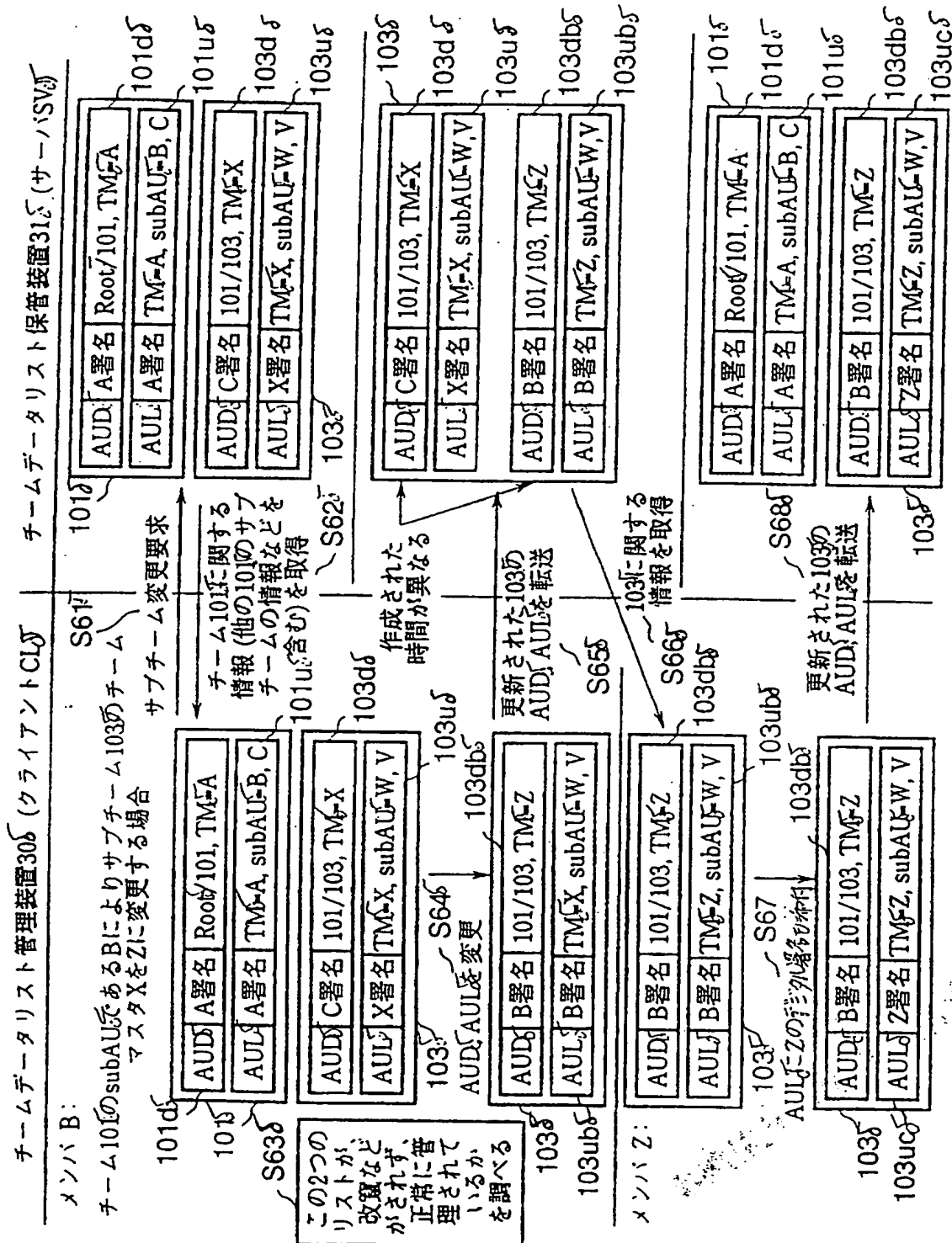




*This Page Blank (uspto)*



図 4 5



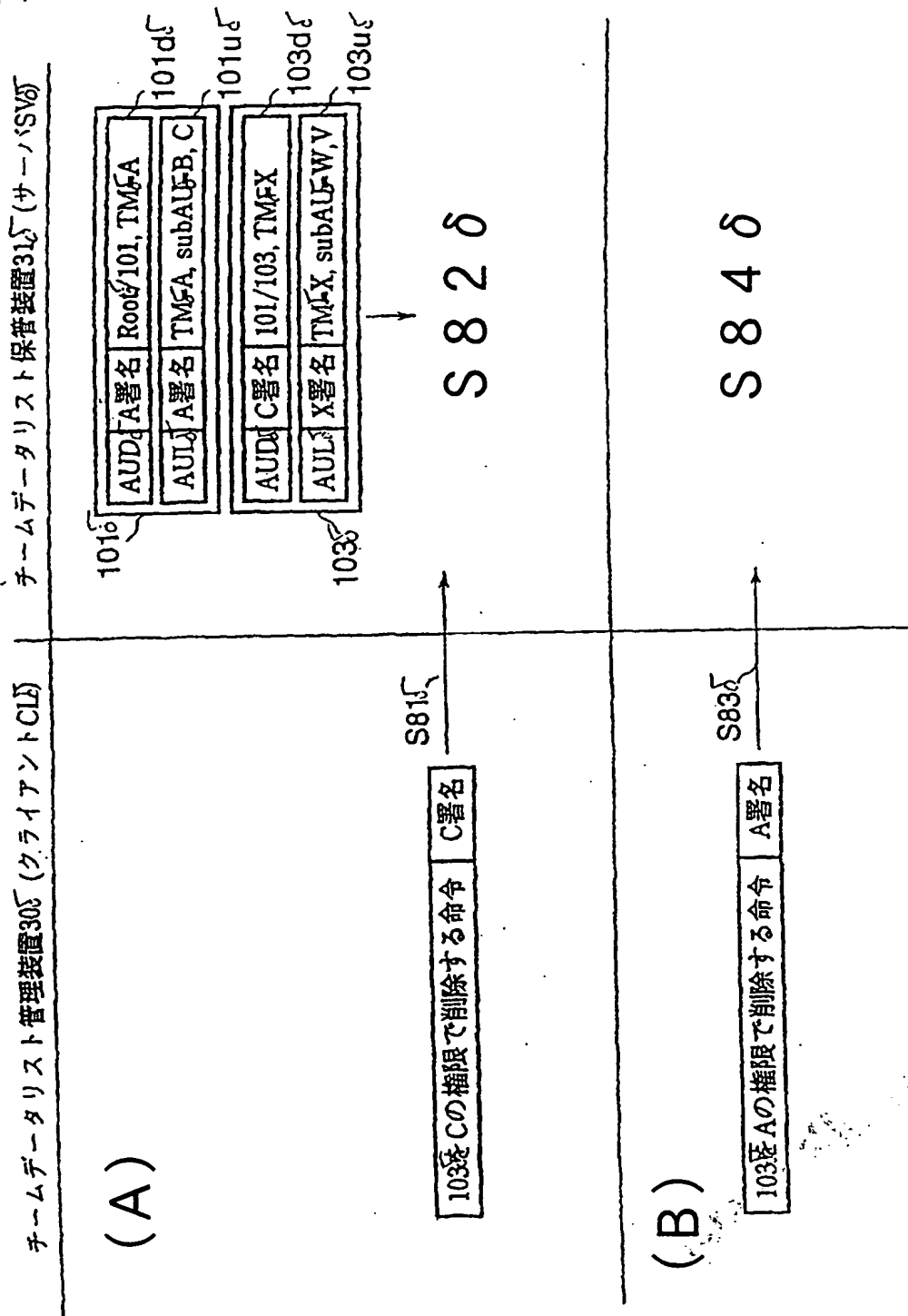
*This Page Blank (uspto)*



*This Page Blank (uspto)*

45 / 73

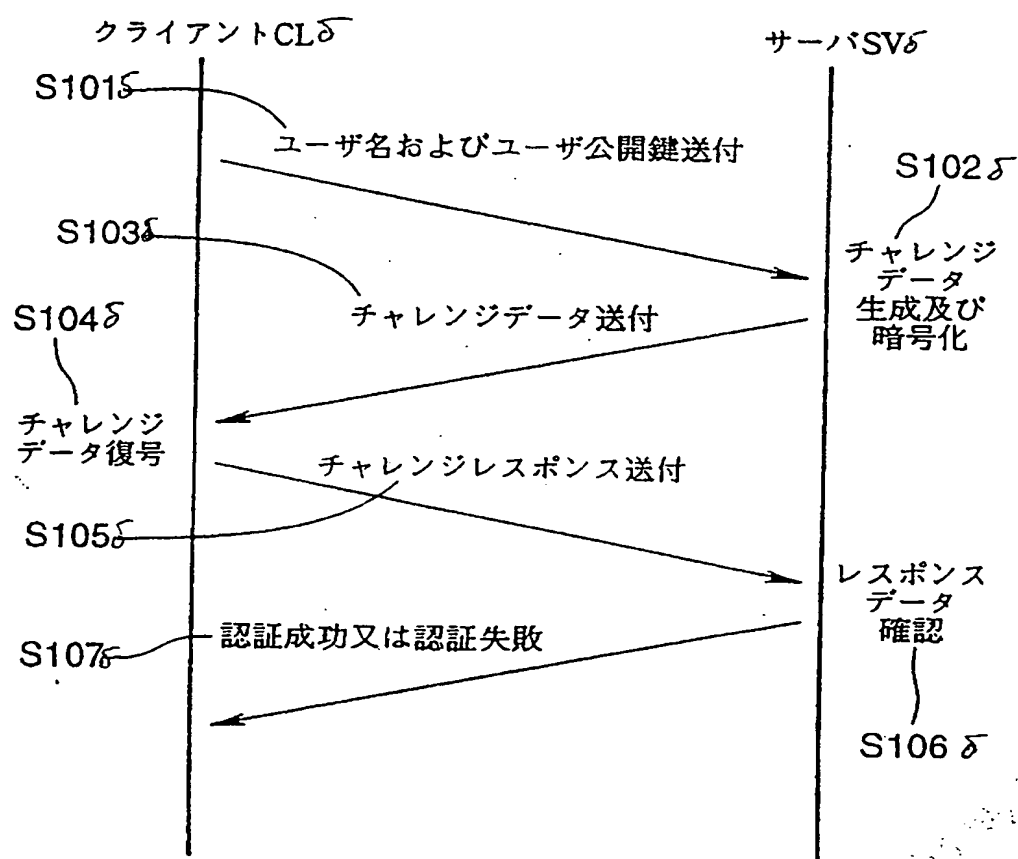
図 47



*This Page Blank (uspto)*

46/7 3

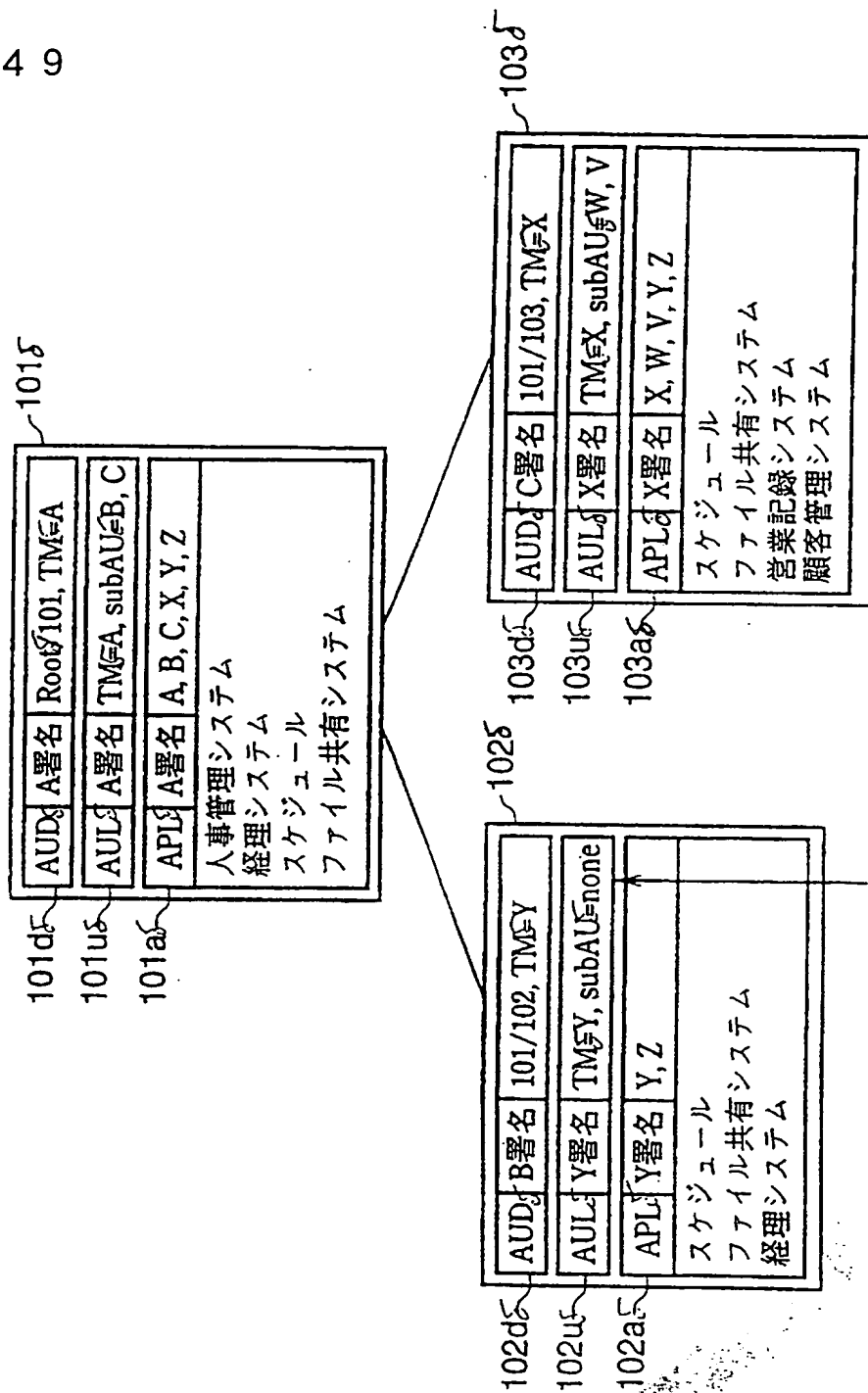
図 4 8



This Page Blank (uspto)



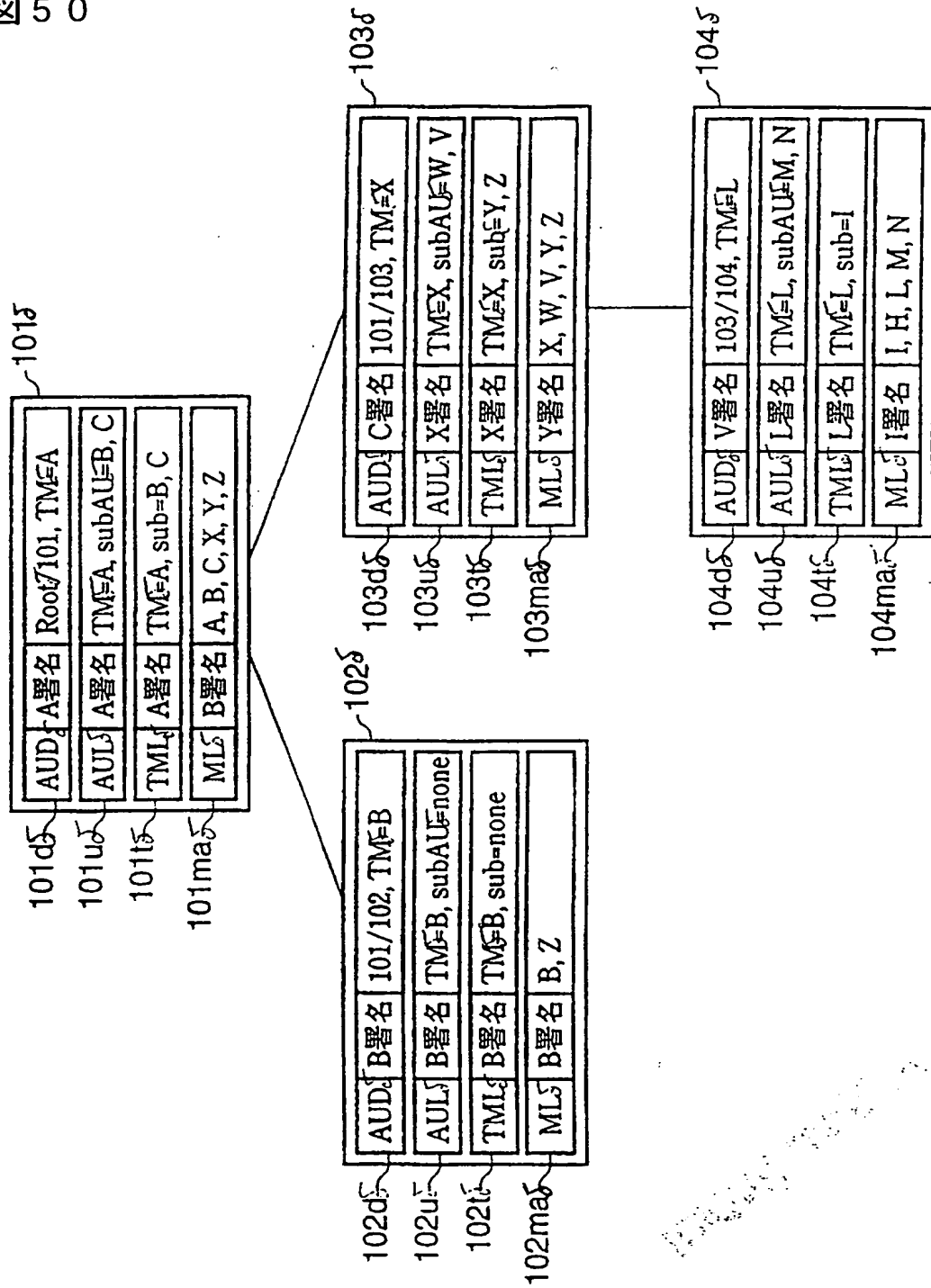
図 4 9



*This Page Blank (uspto)*

48/73

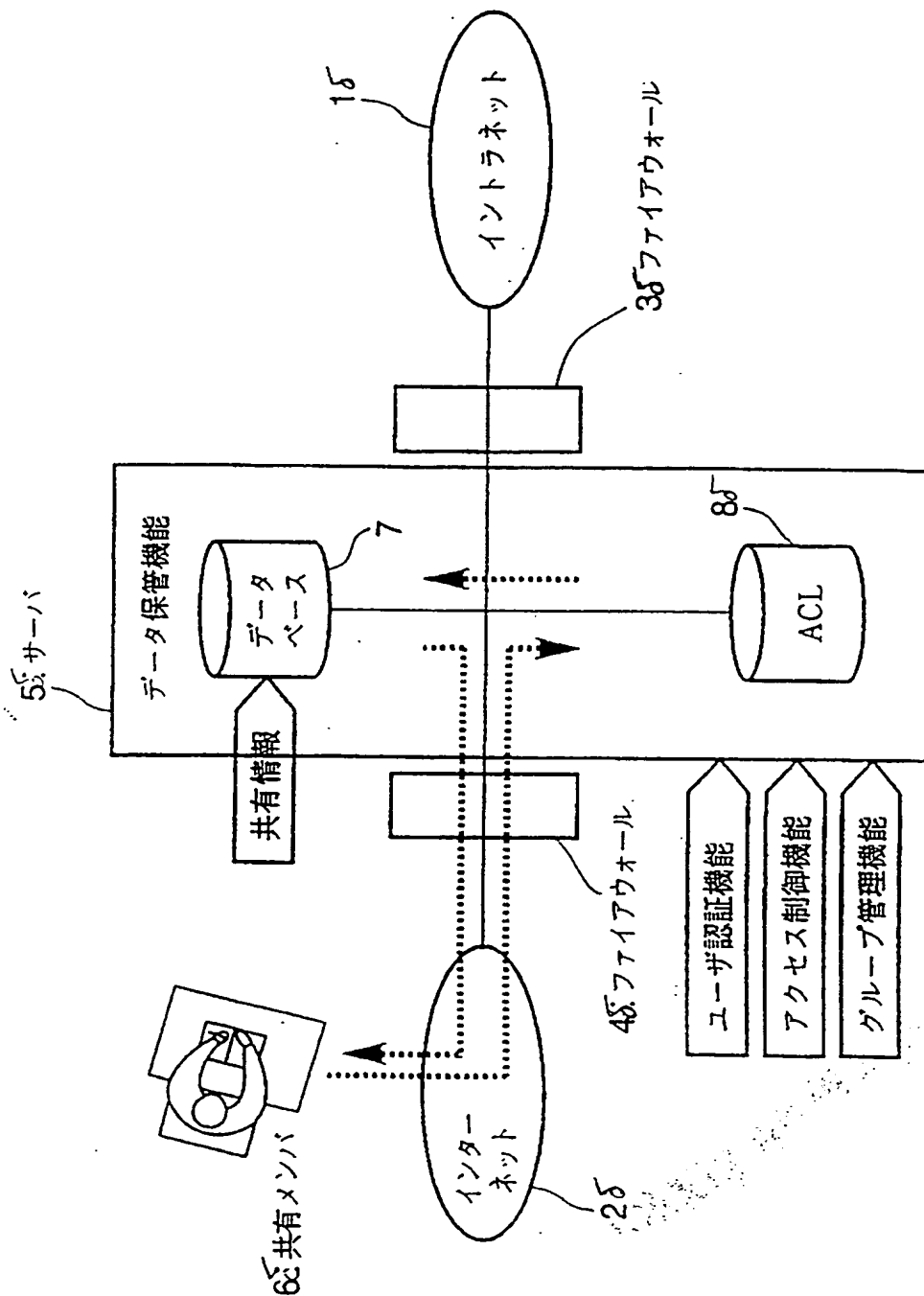
図 50



*This Page Blank (uspto)*

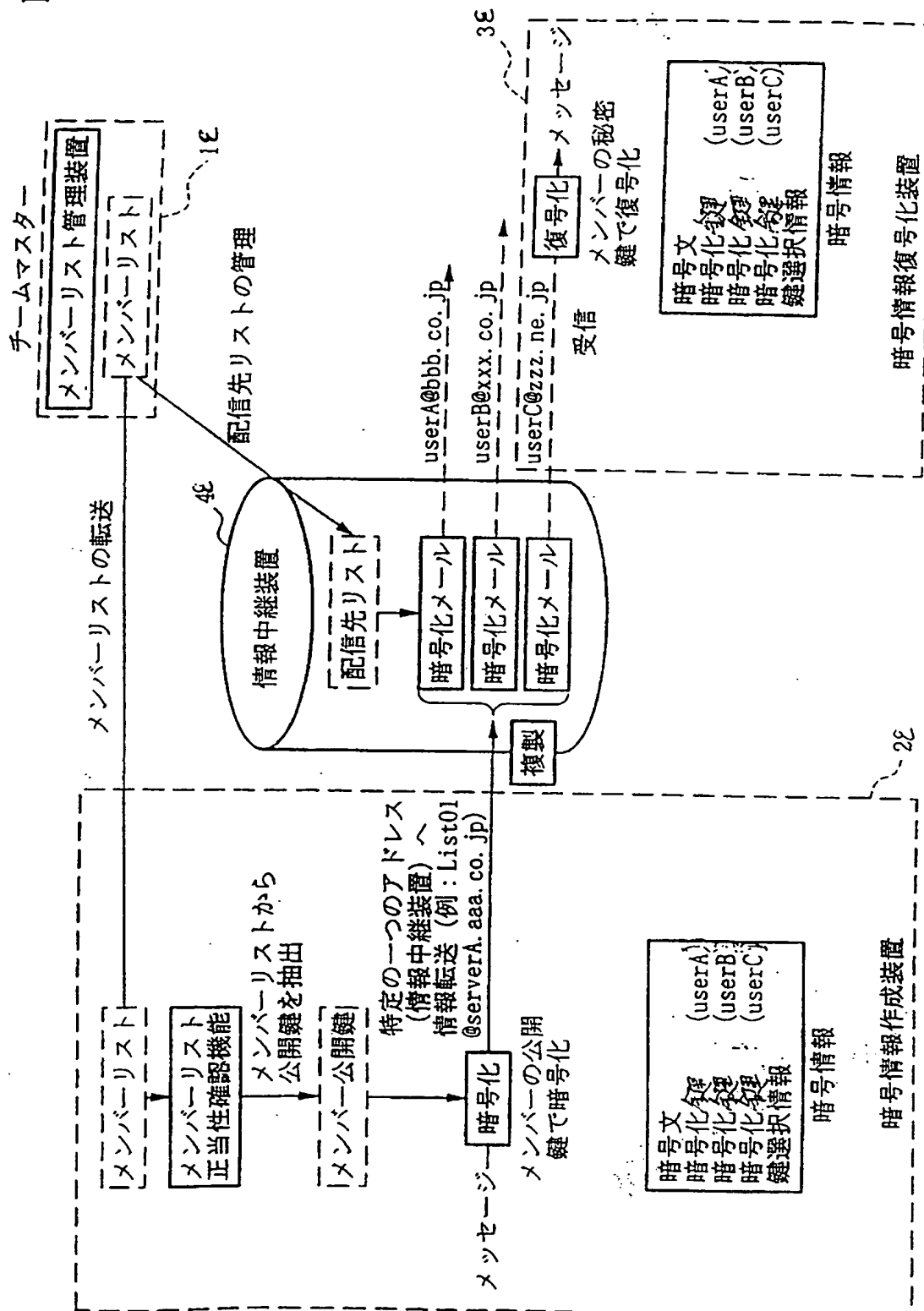
49/7 3

図 5 1



*This Page Blank (uspto)*

圖 5 2



This Page Blank (uspto)



51/7 3

図 5 3

メンバーリスト

|                     |
|---------------------|
| チーム101E             |
| メンバーX               |
| メンバーY<br>:<br>メンバーB |
| Xのデジタル署名            |

図 5 4

チームマスターリスト

|          |      |
|----------|------|
| チーム101E  |      |
| メンバーX    | マスター |
| メンバーY    | サブ   |
| メンバーZ    | サブ   |
| Xのデジタル署名 |      |

メンバーリスト

|                     |
|---------------------|
| チーム101E             |
| メンバーX               |
| メンバーY<br>:<br>メンバーB |
| Xのデジタル署名            |

*This Page Blank (uspto)*

52/7 3

図 5 5

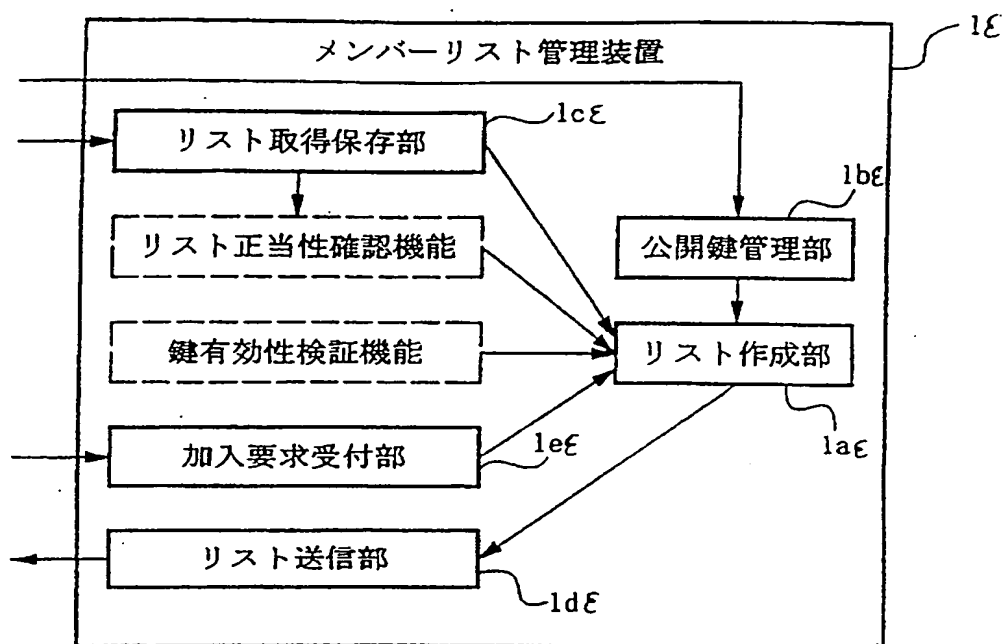
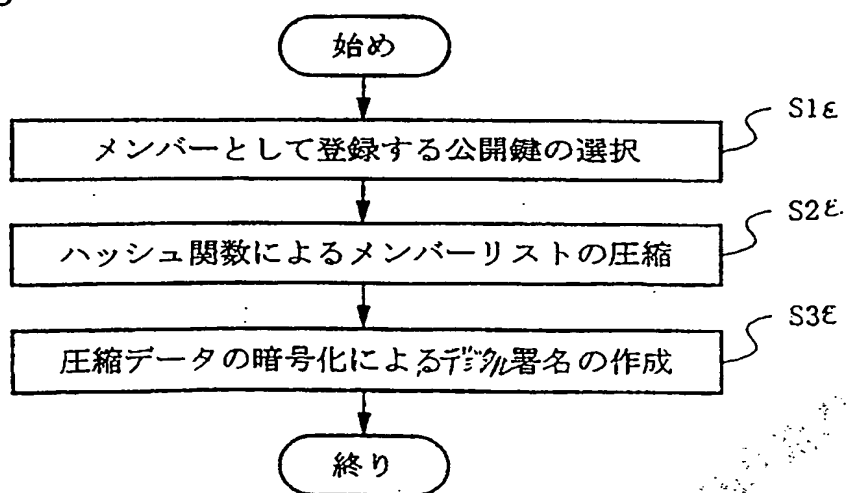
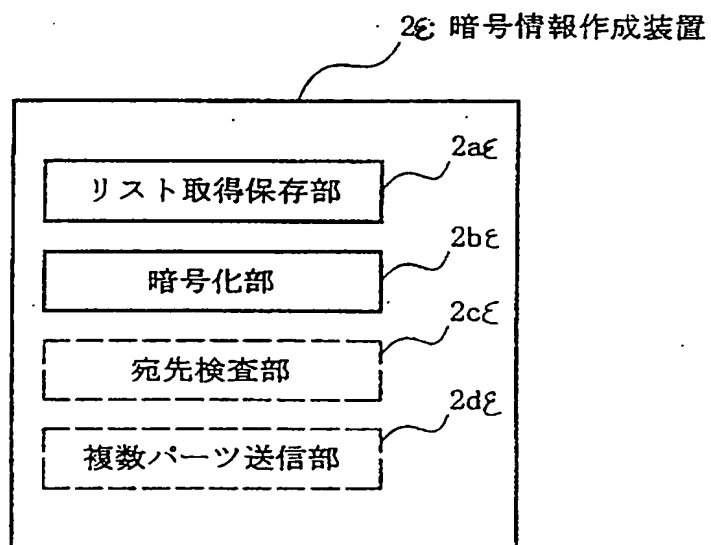


図 5 6



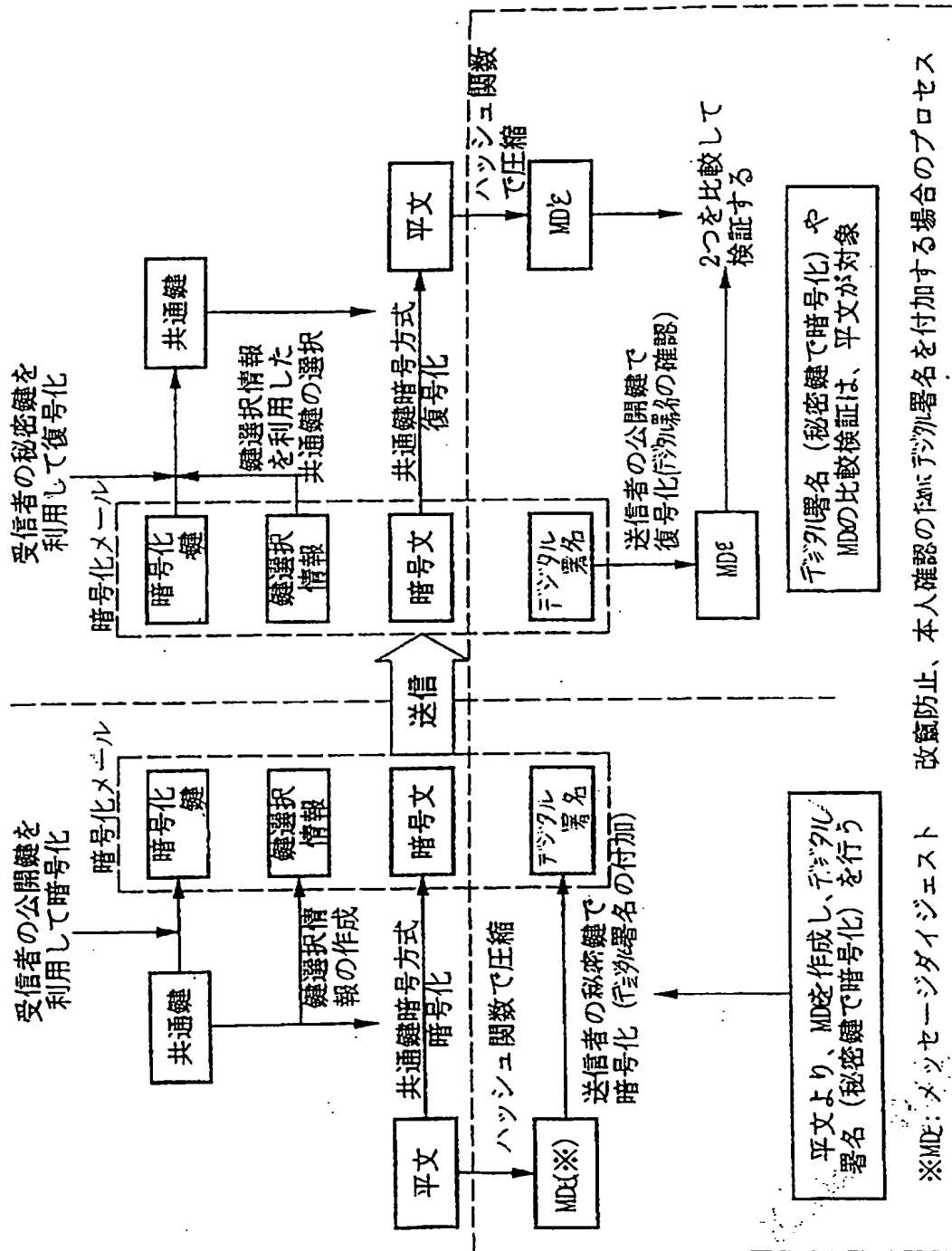
*This Page Blank (uspto)*

図 5 7



's Page Blank (uspto)

图 5 8

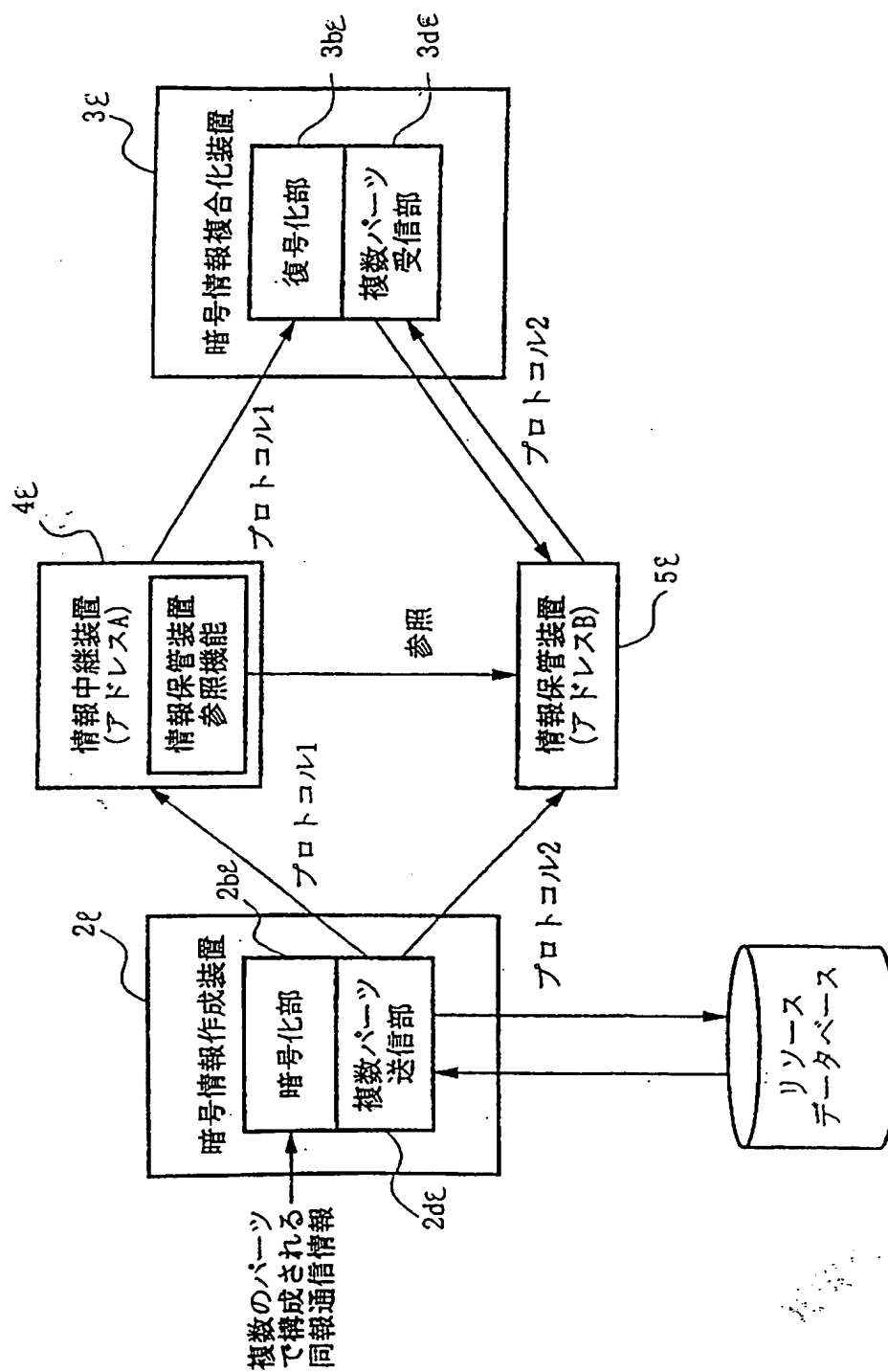


*This Page Blank (uspto)*



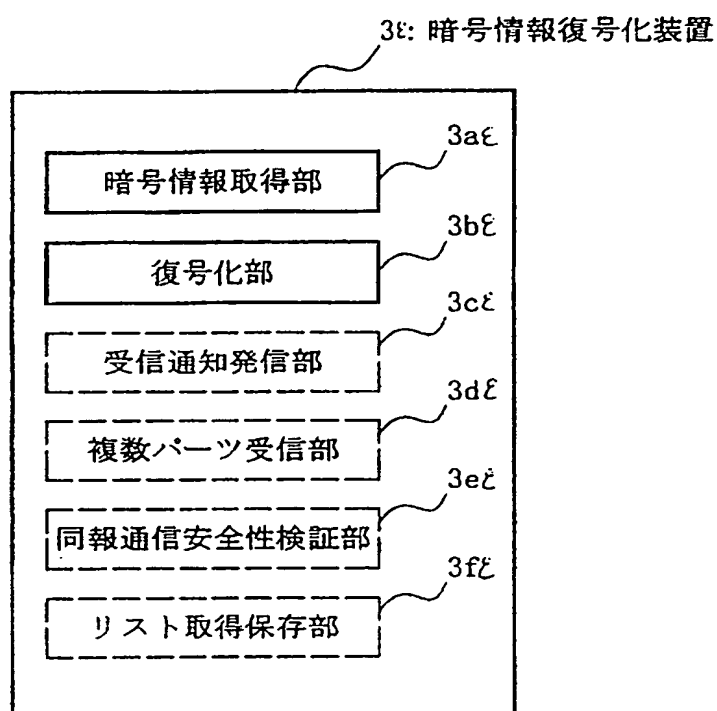
55 / 7 3

図 5 9



*This Page Blank (uspto)*

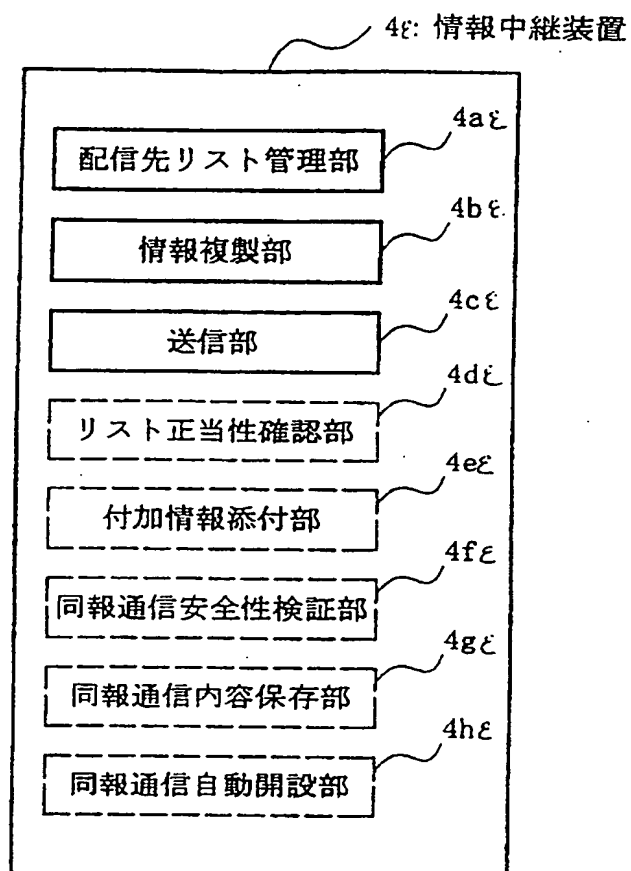
図 6 0



*This Page Blank (uspto)*

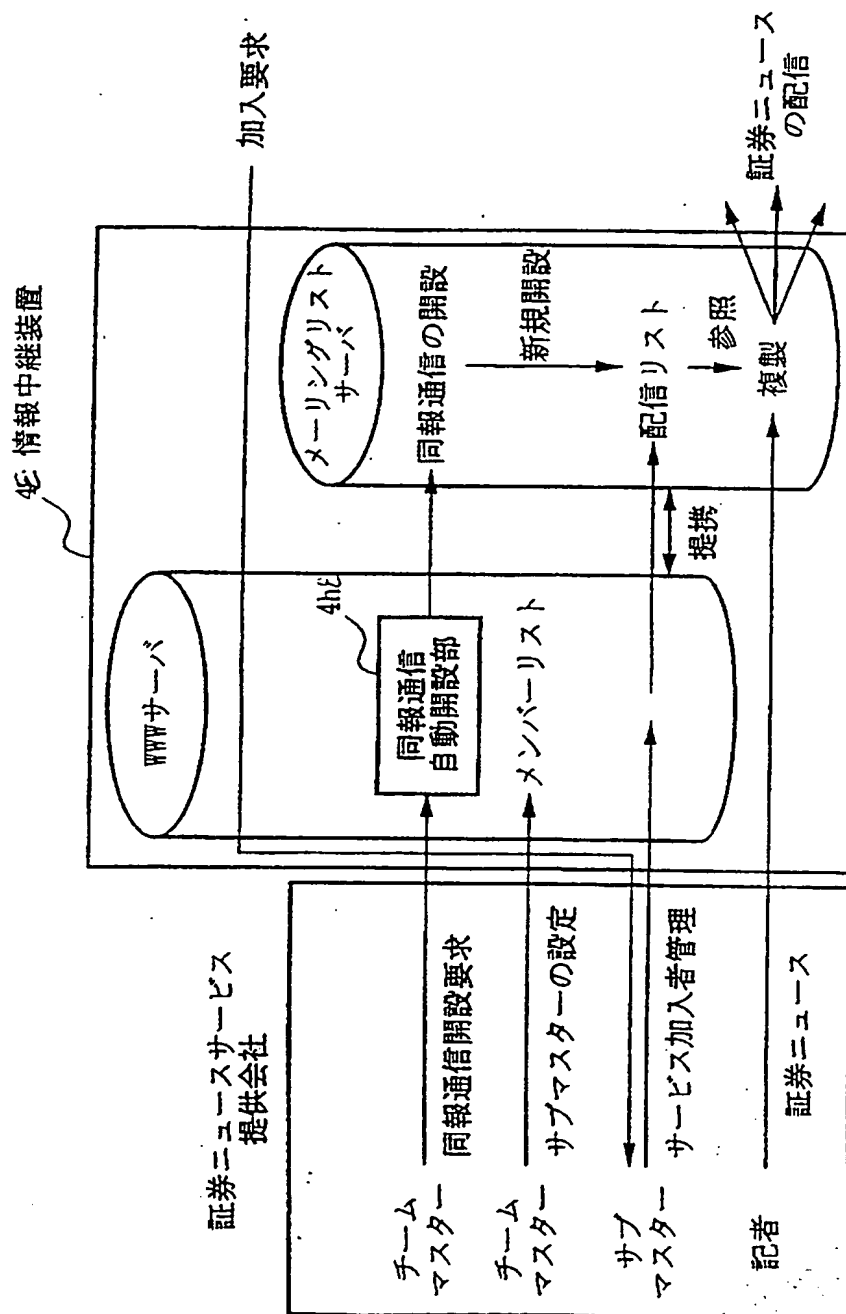
57/7 3

図 6 1



*This Page Blank (uspto)*

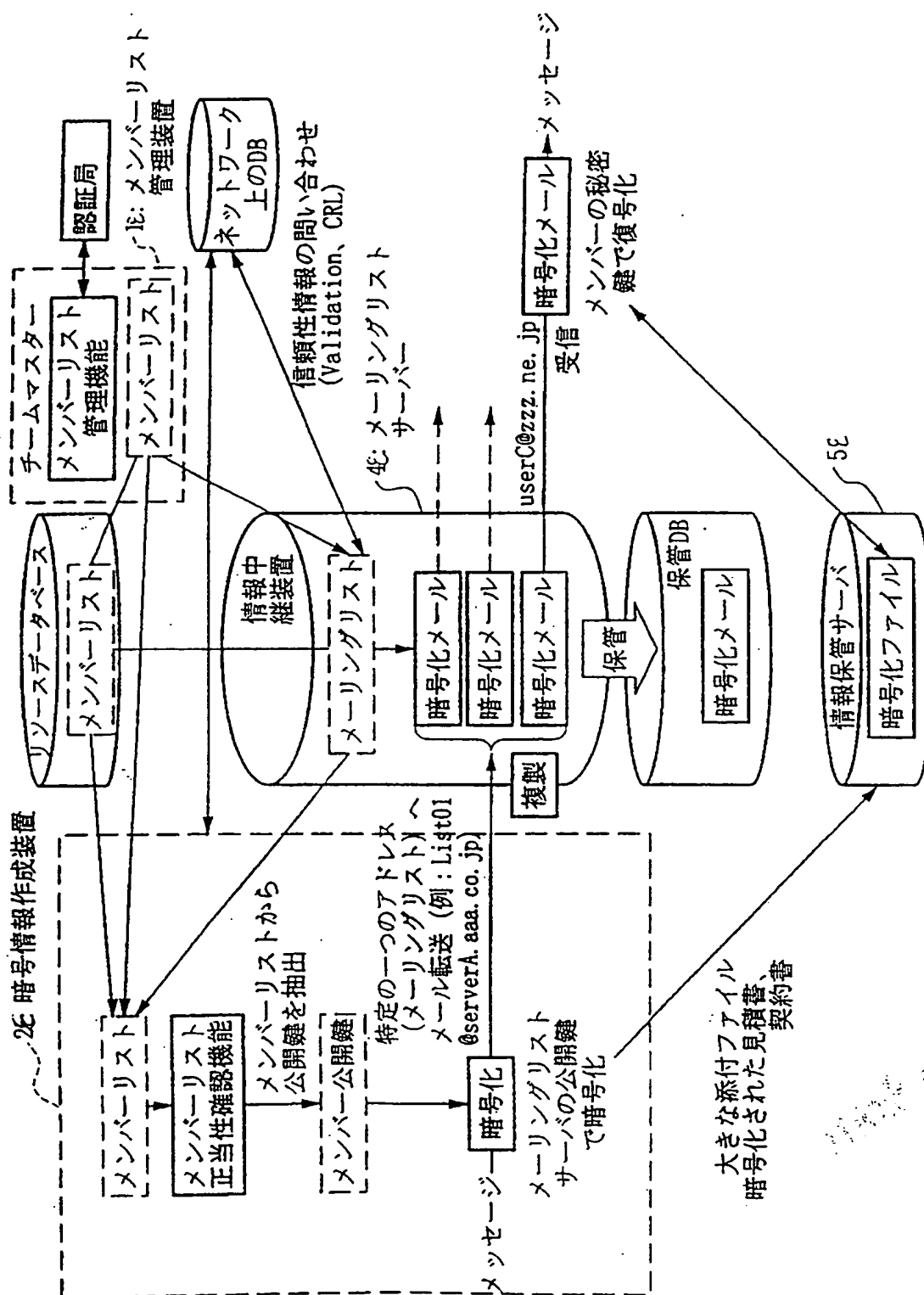
図 6 2



This Page Blank



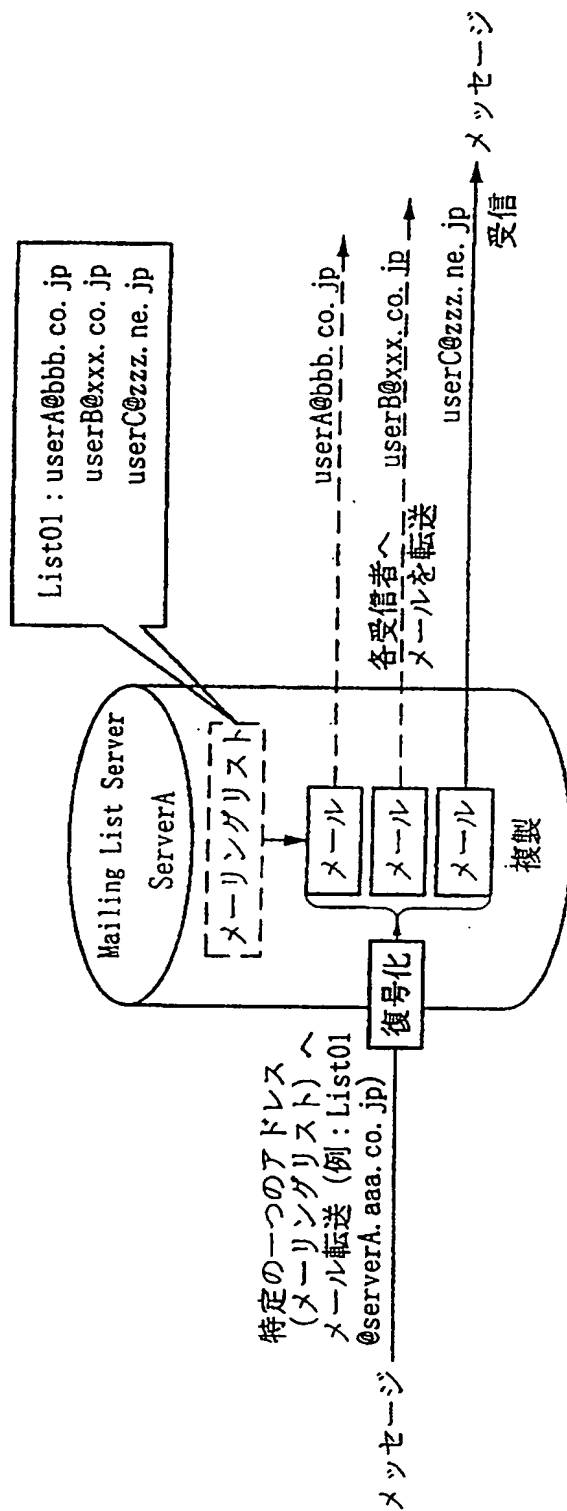
图 6 3



~~This~~ Page Blank (uspto)

60/73

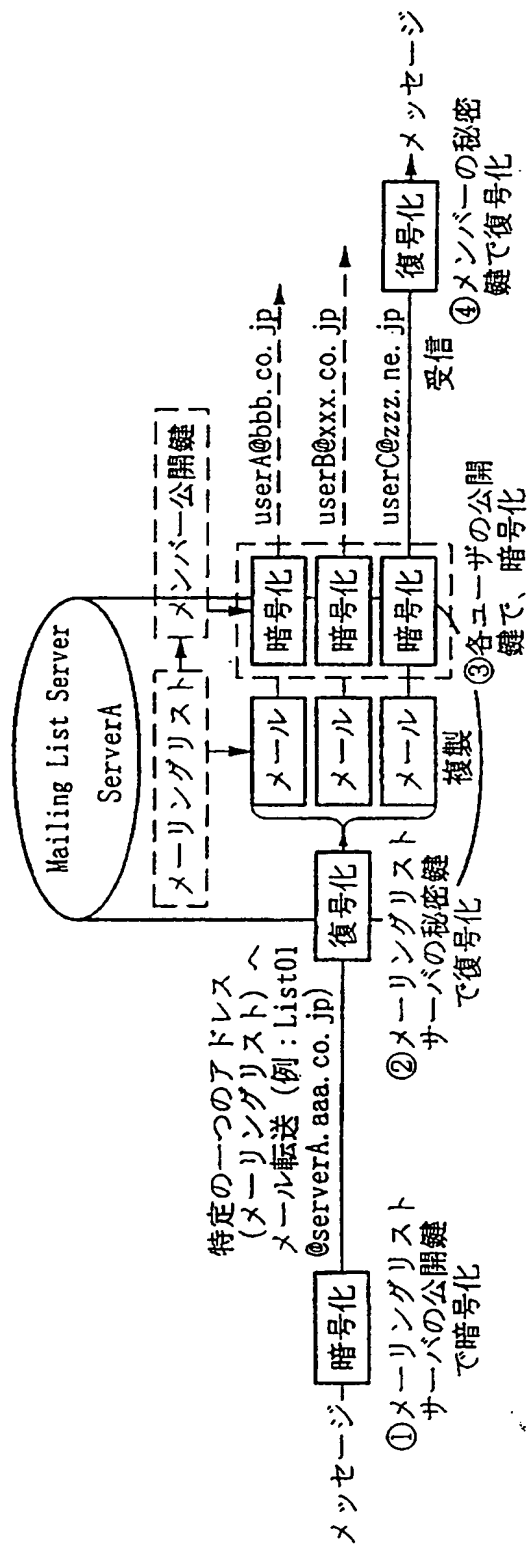
図 6 4



*This Page Blank (uspto)*

61/7 3

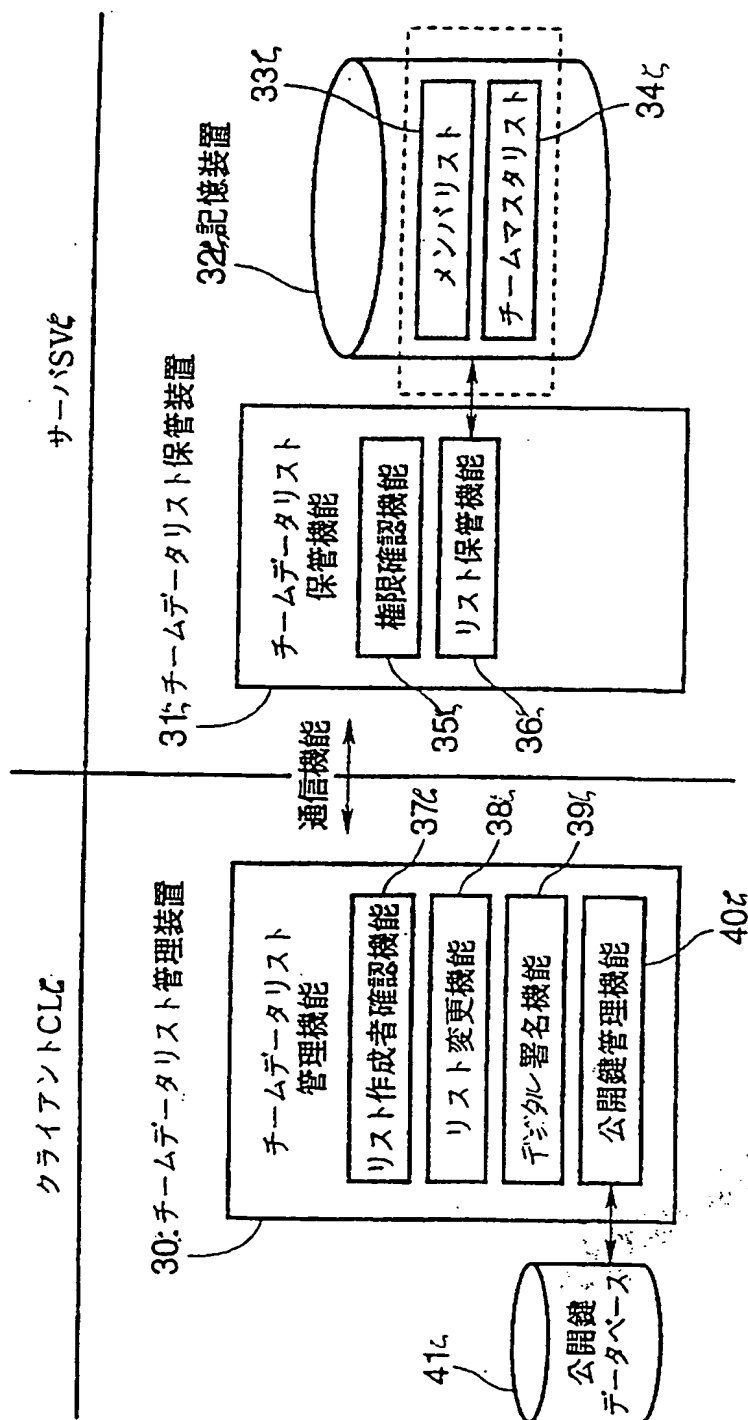
図 6 5



*This Page Blank (uspto)*

62/7 3

図 6 6

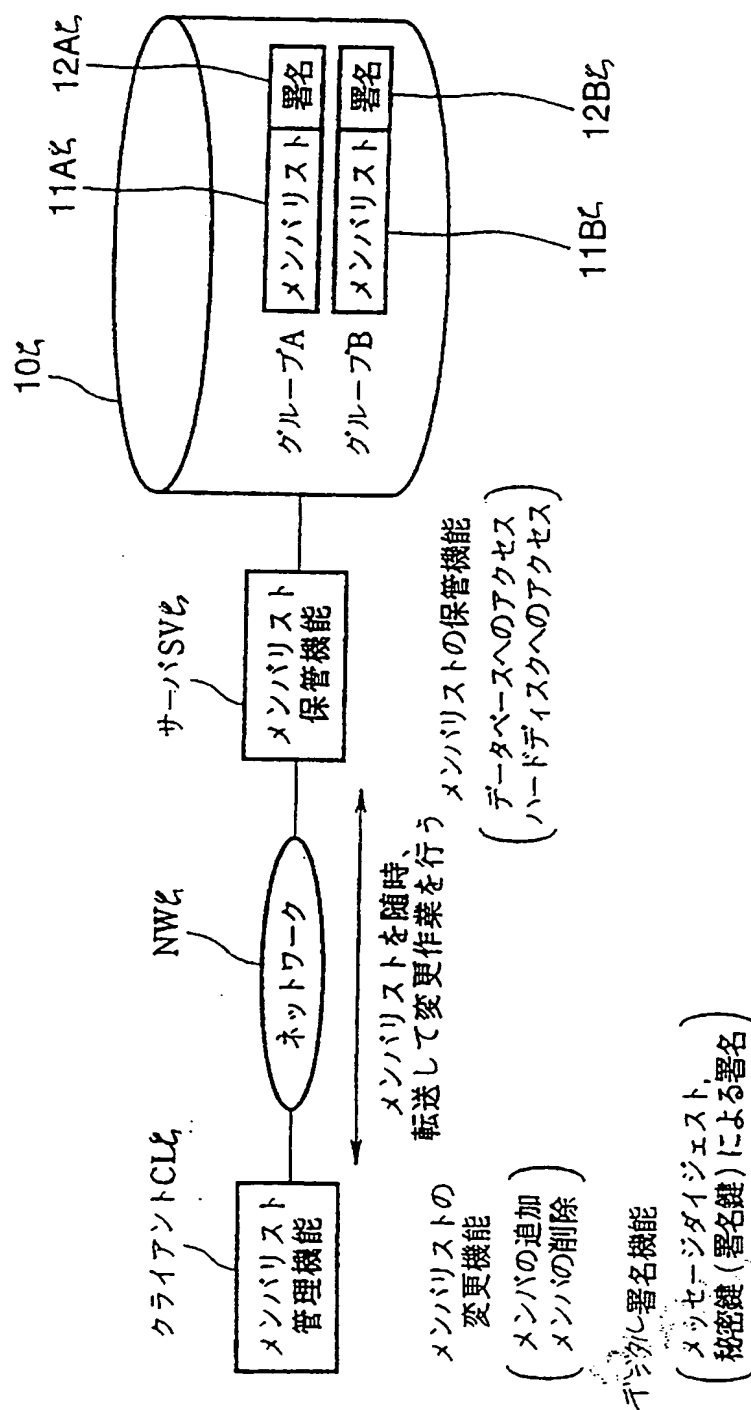


*This Page Blank (uspto)*



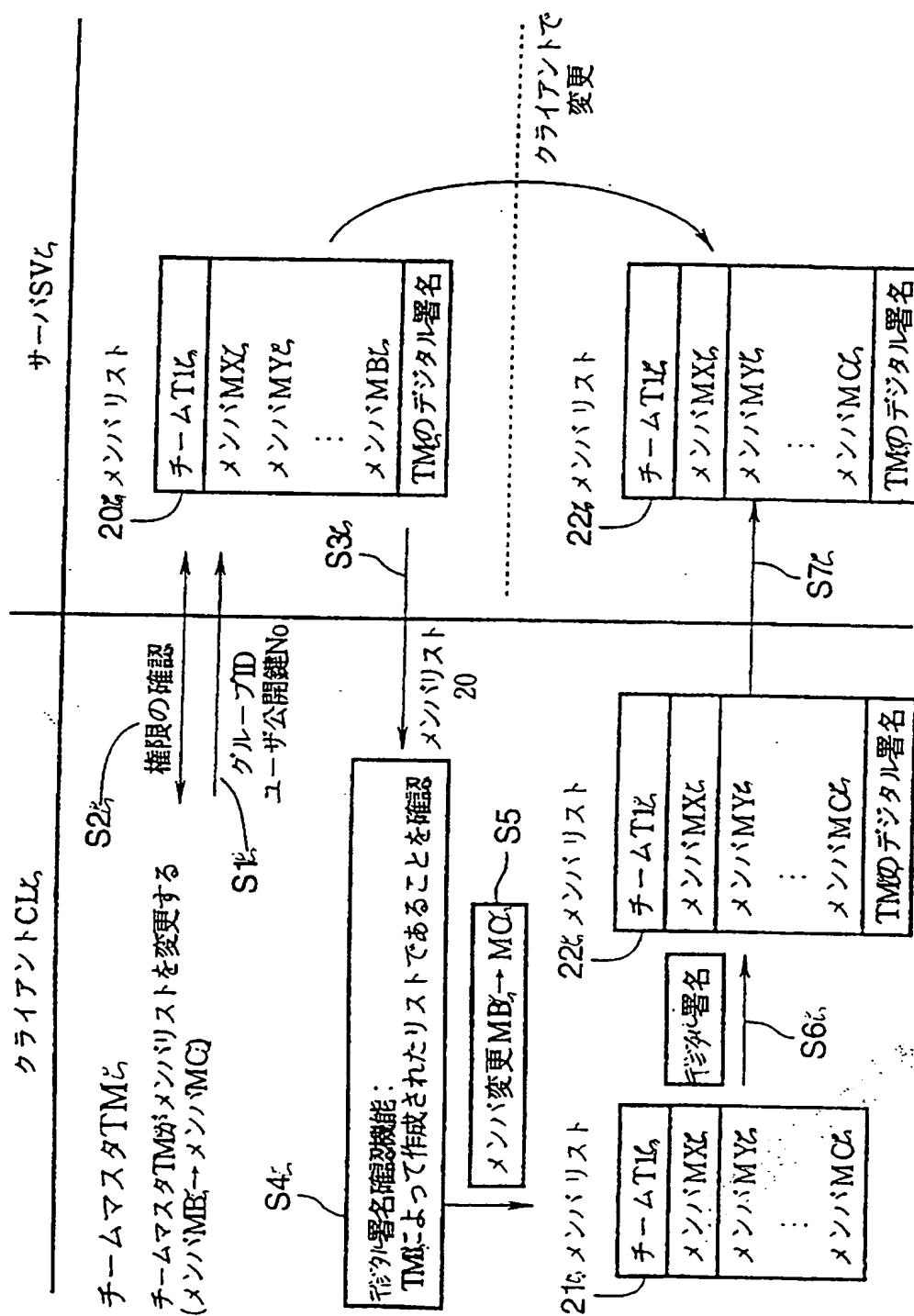
63/7 3

図 6 7



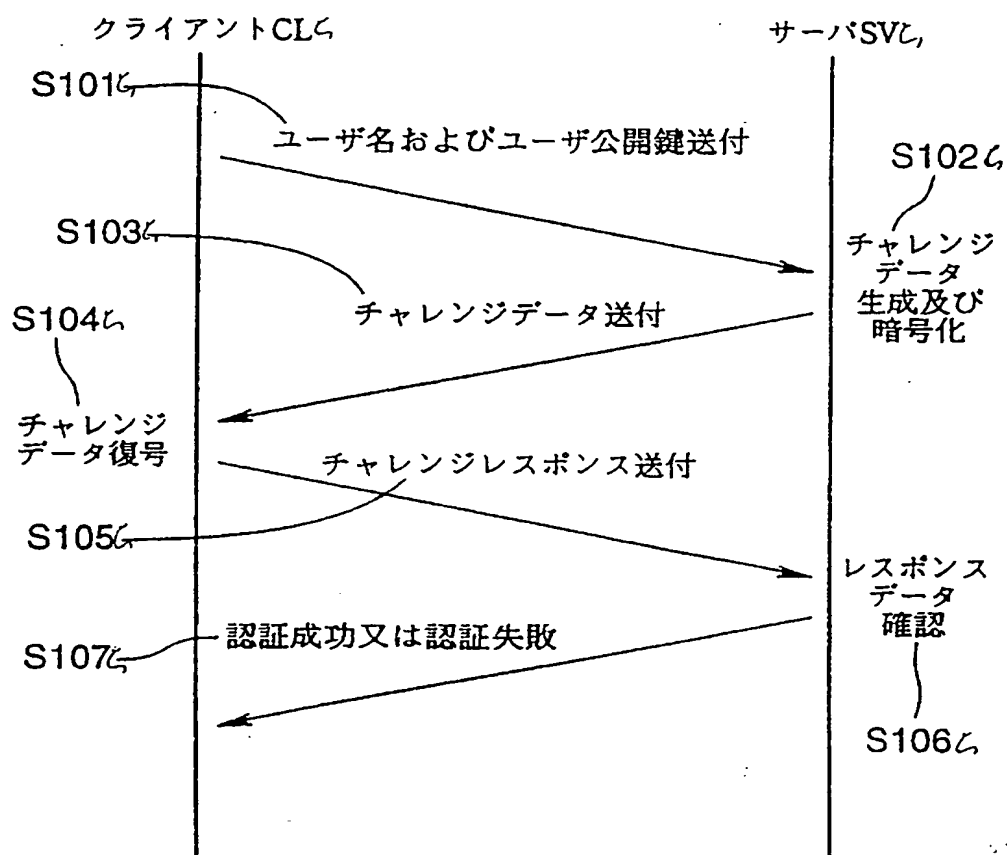
*This Page Blank (uspto)*

図 6 8



*This Page Blank (uspto)*

図 6 9



*This Page Blank (uspto)*

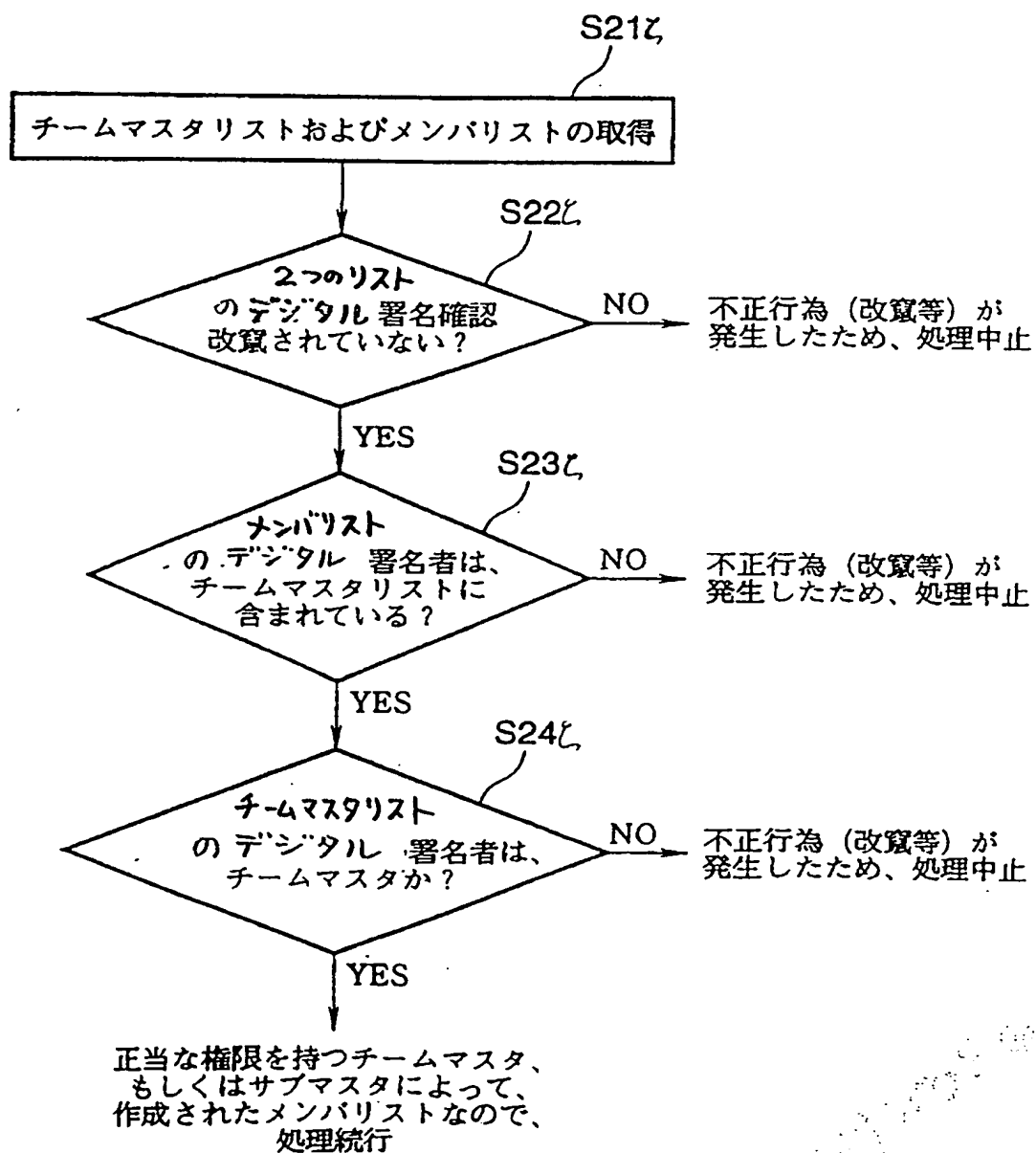


*This Page Blank (uspto)*



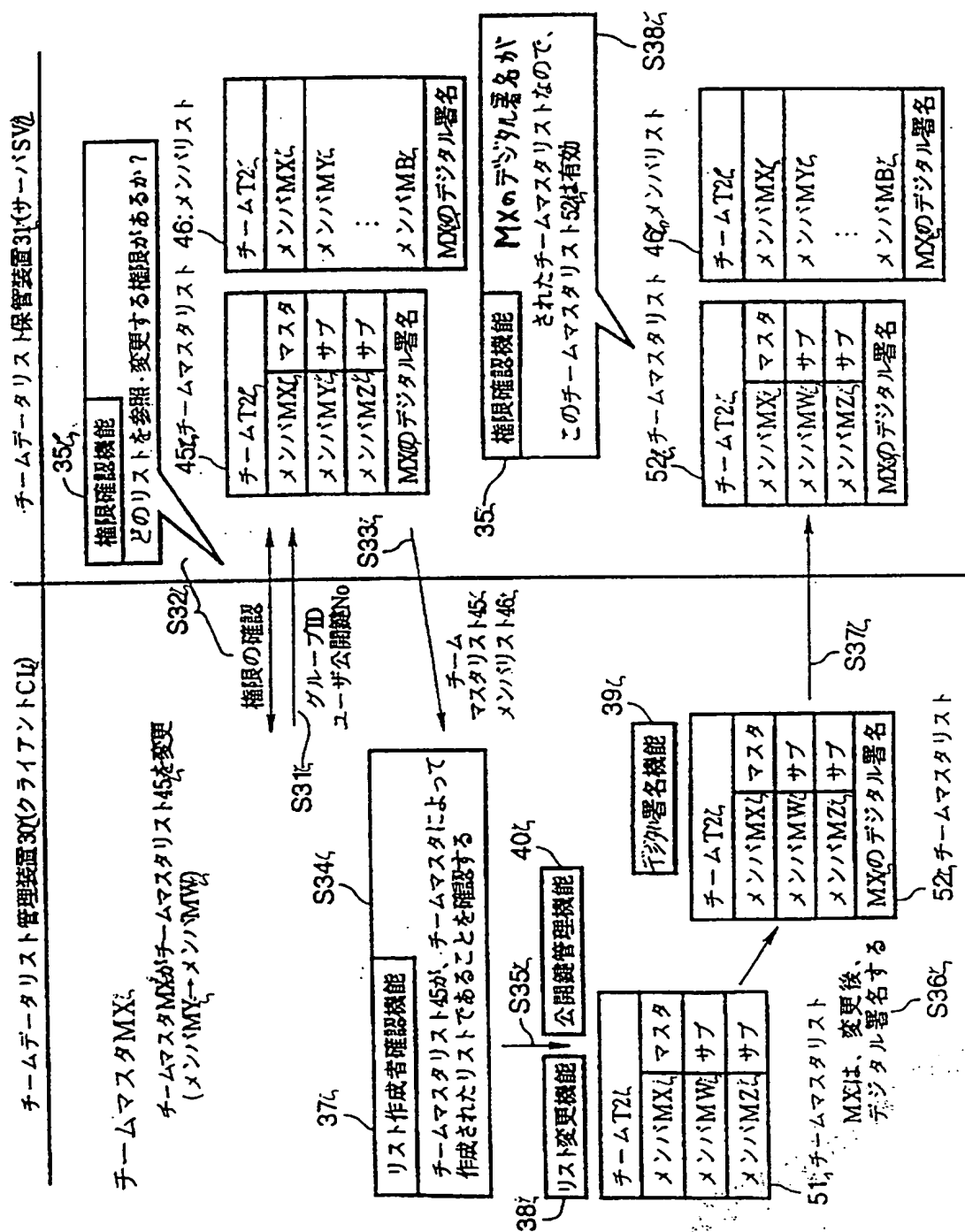
67/7 3

図 7 1



*This Page Blank (uspto)*

图 7 2



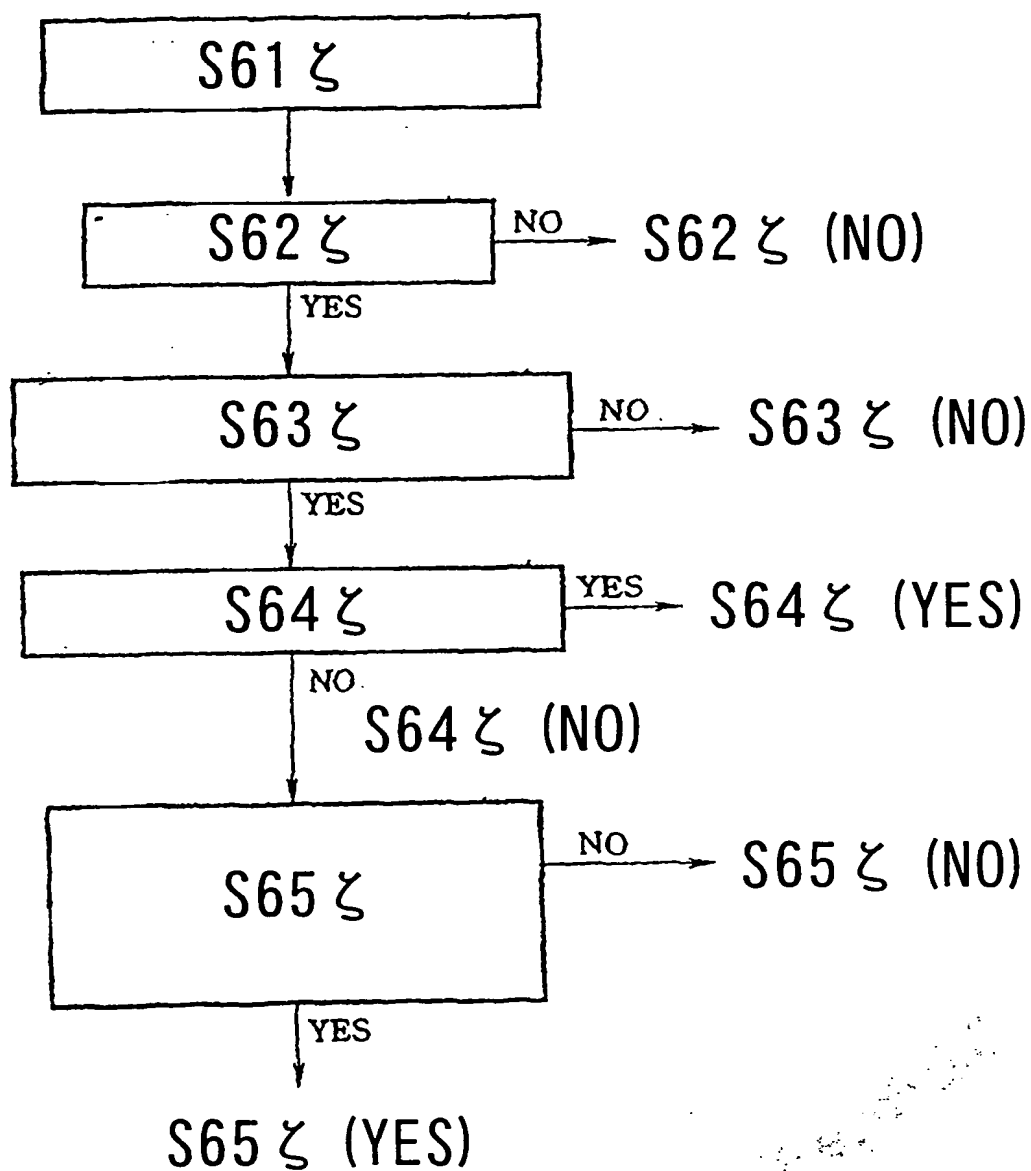
*This Page Blank (uspto)*



*This Page Blank (uspto)*

70 / 73

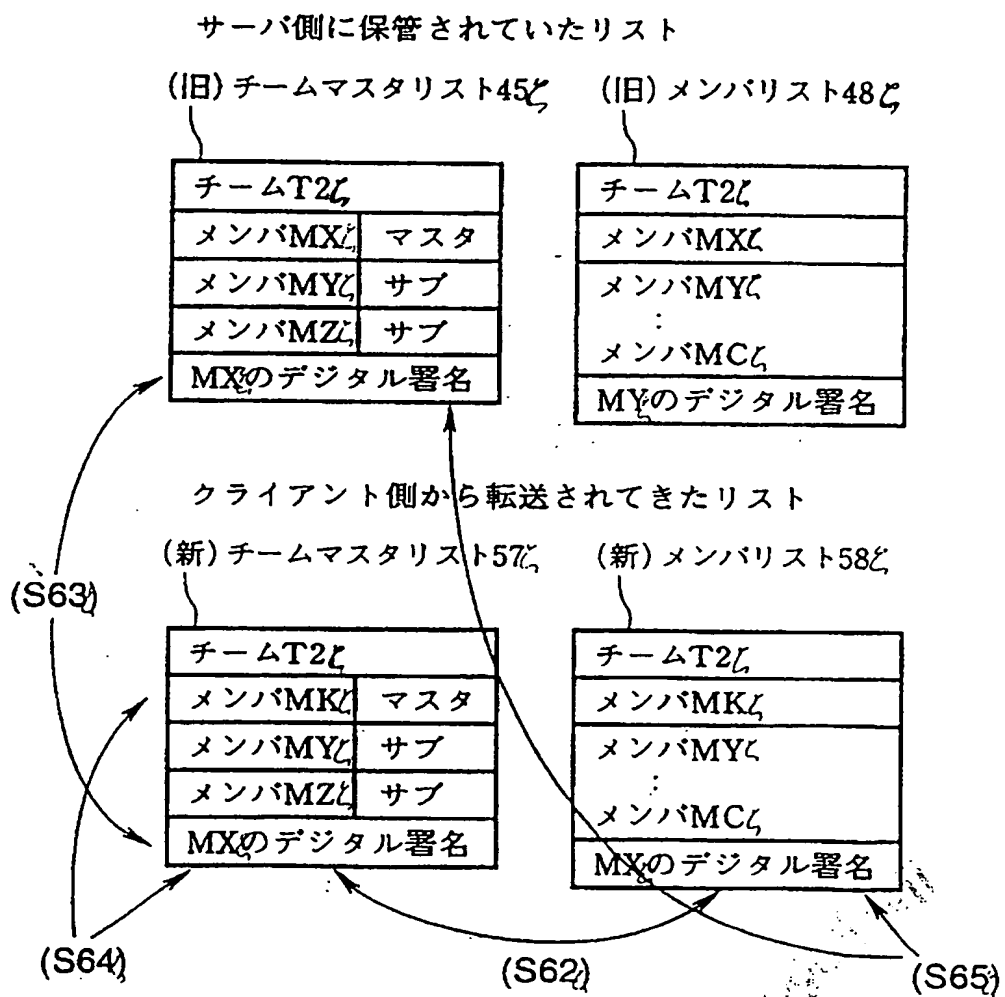
図 7 4



This Page Blank (uspto)



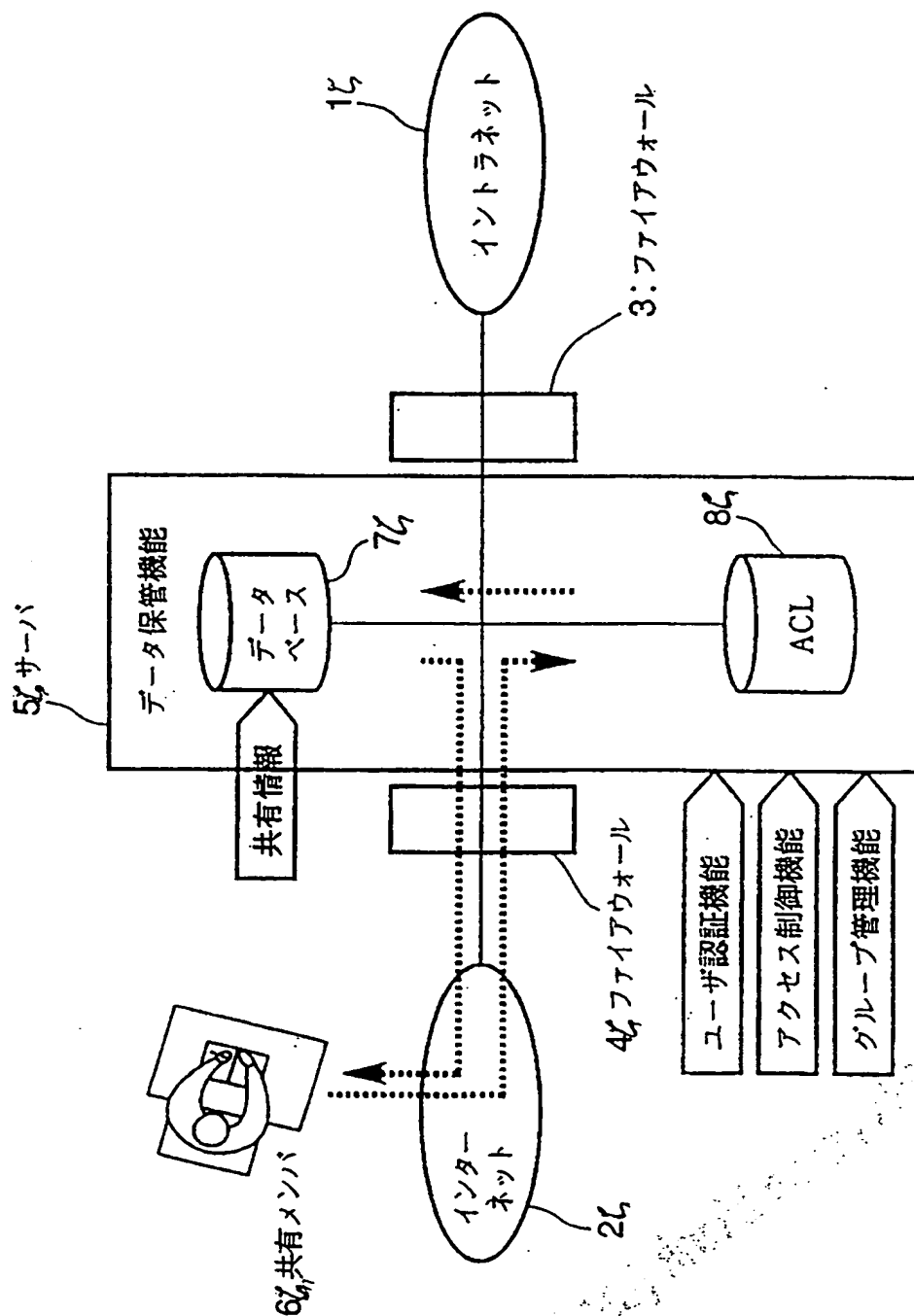
図 7 5



*This Page Blank (uspto)*

72/7 3

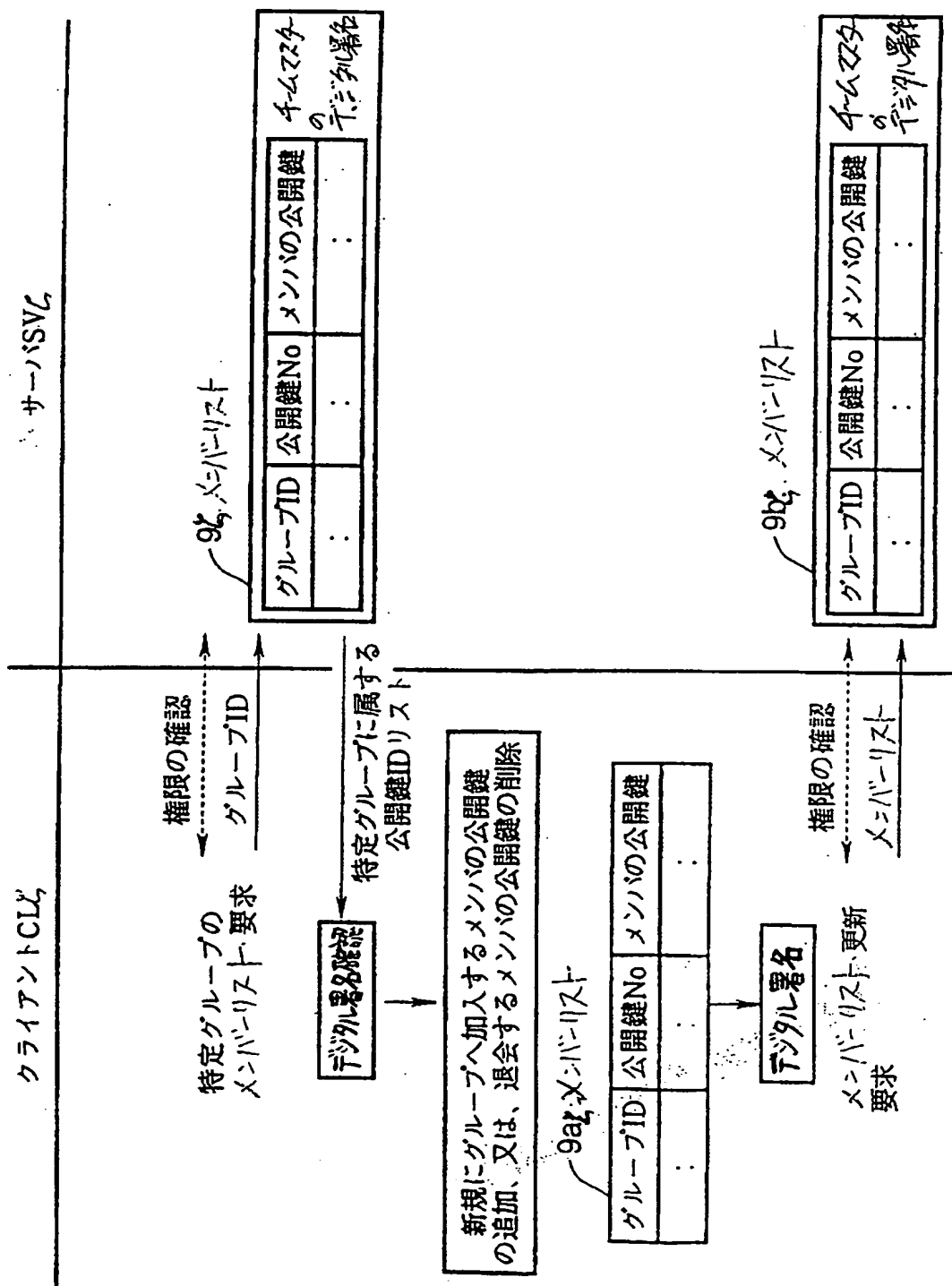
図 7 6



*This Page Blank (usp10)*

73/7 3

図 7 7



***This Page Blank (uspto)***

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/02510

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>6</sup> H04L9/08, H04L9/32, G09C1/00, G06F15/40

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>6</sup> H04L9/08, H04L9/32, G09C1/00, G06F15/40

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1999

Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
|-----------|--|-----------------------|
| Y         | Masahiro Mitsuyasu, Eiji Okamoto, "Kagi haisou, kagi kanri to ninshou"<br>bit, Vol. 28, No. 8 (8. 1996) Pages 87 to 95                               | 1-17, 51-60           |
| Y         | APPLIED CRYPTOGRAPHY SECOND EDITION,<br>"3.1 Key Exchange" (U.S.)<br>John Wiley & Sons, Inc., (1996) Pages 47 to 52                                  | 1-17, 51-60           |
| Y         | JP, 10-13403, A (NEC Corp.),<br>16 January, 1998 (16. 01. 98),<br>Full text ; Figs. 1 to 7 (Family: none)  | 18-106                |
| Y         | JP, 7-200617, A (Nippon Telegraph & Telephone Corp.),<br>4 August, 1995 (04. 08. 95),<br>Full text ; Figs. 1 to 9 (Family: none)                     | 18-27, 61-68          |
| Y         | JP, 10-40155, A (Fujitsu Ltd.),<br>13 February, 1998 (13. 02. 98),<br>Par. Nos. [0022] to [0024], [0027] to [0030] ;<br>Figs. 1 to 15 (Family: none) | 18-60, 96-106         |

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

|   |  |
|---|--|
| * Special categories of cited documents:  | "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  |
| "A" document defining the general state of the art which is not considered to be of particular relevance  | "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone   |
| "E" earlier document but published on or after the international filing date  | "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" document member of the same patent family  |
| "O" document referring to an oral disclosure, use, exhibition or other means  |  |
| "P" document published prior to the international filing date but later than the priority date claimed  |  |

Date of the actual completion of the international search  
18 August, 1999 (18. 08. 99)Date of mailing of the international search report  
31 August, 1999 (31. 08. 99)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/02510

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
|-----------|--|-----------------------|
| Y         | JP, 7-245605, A (Fujitsu Ltd.),<br>19 September, 1995 (19. 09. 95),<br>Full text ; Figs. 1 to 10<br>& GB, 2287160, A & US, 5642420, A                | 73-91                 |
| Y         | JP, 9-252323, A (Sony Corp.),<br>22 September, 1997 (22. 09. 97),<br>Par. Nos. [0028] to [0033] ; [0040] to [0052] ;<br>Figs. 1 to 10 (Family: none) | 28-50, 78-91          |



## 国際調査報告

国際出願番号 PCT/J P 99/02510

|   |   |  |
|---|---|--|
| A. 発明の属する分野の分類 (国際特許分類 (IPC))   |   |  |
| Int. Cl. <sup>8</sup> H04L9/08, H04L9/32, G09C1/00, G06F 15/40  |   |  |
| B. 調査を行った分野   |   |  |
| 調査を行った最小限資料 (国際特許分類 (IPC))  |   |  |
| Int. Cl. <sup>8</sup> H04L9/08, H04L9/32, G09C1/00, G06F 15/40  |   |  |
| 最小限資料以外の資料で調査を行った分野に含まれるもの  |   |  |
| 日本国実用新案公報 1922-1996年<br>日本国公開実用新案公報 1971-1999年<br>日本国登録実用新案公報 1994-1999年<br>日本国実用新案登録公報 1996-1999年  |   |  |
| 国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)   |   |  |
| C. 関連すると認められる文献   |   |  |
| 引用文献の<br>カテゴリー*   | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示   | 関連する<br>請求の範囲の番号   |
| Y   | 満保 雅浩, 岡本 栄司, "鍵配送、鍵管理と認証"<br>bit, Vol. 28, No. 8 (8. 1996) 第87-95頁                                       | 1-17, 51-60  |
| Y   | APPLIED CRYPTOGRAPHY SECOND EDITION,<br>"3.1 Key Exchange" (米)<br>John Wiley & Sons, Inc., (1996) 第47-52頁 | 1-17, 51-60  |
| Y   | JP, 10-13403, A (日本電気株式会社)<br>16.1月. 1998 (16.01.98)<br>全文, 第1-7図 (ファミリーなし)                               | 18-106   |
| <input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。   |   |  |
| * 引用文献のカテゴリー<br>「A」特に関連のある文献ではなく、一般的技術水準を示すもの<br>「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの<br>「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)<br>「O」口頭による開示、使用、展示等に言及する文献<br>「P」国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献<br>「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの<br>「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの<br>「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの<br>「&」同一パテントファミリー文献 |   |  |
| 国際調査を完了した日<br>18.08.99  |   | 国際調査報告の発送日<br>31.08.99                                   |
| 国際調査機関の名称及びあて先<br>日本国特許庁 (ISA/J P)<br>郵便番号 100-8915<br>東京都千代田区霞が関三丁目4番3号  |   | 特許庁審査官 (権限のある職員)<br>青木 重徳 印<br>電話番号 03-3581-1101 内線 3576 |

## C (続き) . 関連すると認められる文献

| 引用文献の<br>カテゴリー* | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示   | 関連する<br>請求の範囲の番号 |
|-----------------|---|------------------|
| Y               | JP, 7-200617, A (日本電信電話株式会社)<br>4. 8月. 1995 (04. 08. 95)<br>全文, 第1-9図 (ファミリーなし)   | 18-27, 61-68     |
| Y               | JP, 10-40155, A (富士通株式会社)<br>13. 2月. 1998 (13. 02. 98)<br>第 [0022] - [0024] 段落, 第 [0027] - [0030] 段落,<br>第1-15図 (ファミリーなし) | 18-60, 96-106    |
| Y               | JP, 7-245605, A (富士通株式会社)<br>19. 9月. 1995 (19. 09. 95)<br>全文, 第1-10図<br>& GB, 2287160, A & US, 5642420, A                 | 73-91            |
| Y               | JP, 9-252323, A (ソニー株式会社)<br>22. 9月. 1997 (22. 09. 97)<br>第 [0028] - [0033] 段落, 第 [0040] - [0052] 段落,<br>第1-10図 (ファミリーなし) | 28-50, 78-91     |

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

